OPINNÄYTETYÖ

KEIJO RUONALA 2011

KUNNAN TIETOTURVAJOHTAMINEN – TIETOTURVAN JALKAUTTAMINEN OSAKSI ARKIPÄIVÄN TOIMINTAA

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC

TEKNOLOGIAOSAAMISEN JOHTAMINEN

ROVANIEMEN AMMATTIKORKEAKOULU

TEKNIIKKA JA LIIKENNE

Teknologiaosaamisen johtaminen

Opinnäytetyö YAMK

KUNNAN TIETOTURVAJOHTAMINEN – TIETOTURVAN JALKAUTTAMINEN OSAKSI ARKI-PÄIVÄN TOIMINTAA

Keijo Ruonala

2011

Toimeksiantajana kunta Pohjois-Suomesta

Ohjaajana Veikko Kärnä

Hyväksytty _____ 2011 _____

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC

Tekniikka ja liikenne
Teknologiaosaamisen johtamisen koulutus-ohjelma

Opinnäytetyön tiivistelmä

Tekijä Keijo Ruonala Vuosi 2011

Toimeksiantaja Kunta Pohjois-Suomesta
Työn nimi Kunnan tietoturvajohtaminen – Tietoturvan jalkauttaminen osaksi arkipäivän toimintaa
Sivu- ja liitemäärä 58 + 1

Opinnäytetyöni aiheena on tutkia tietoturvajohtamista tutkimuskohteessa ja kehittää niitä menetelmiä, joilla tietoturvalliset toimintatavat saadaan osaksi henkilöstön päivittäisiä työrutiineja. Muita tutkimusaiheita ovat etätyön ja sähköisen asioinnin kehittämistarpeet tutkimuskohteessa.

Tietoturvastandardi SFS 27001 (2006) ja kunnan omat tietoturvaan liittyvät ohjeet, jotka perustuvat tietoturvastandardiin SFS 17799 (2005), määrittelevät tietoturvallisuuden hallintajärjestelmälle ja tietoturvajohtamiselle asetettavat vaatimukset ja tavoitteet.

Tietoturvajohtamista ja etätyöhön sekä sähköiseen asiointiin liittyviä kehittämistarpeita tutkittiin haastattelemalla tutkimuskohteen osastopäälliköitä. Tutkimustuloksia verrattiin kunnan omiin ohjeisiin ja alan kirjallisuuteen.

Tutkimuksen tuloksena selvisi, että tietoturvaan liittyvät ohjeet ovat standardin SFS 27001 vaatimusten mukaisia. Ohjeet vaativat kuitenkin säännöllistä päivittämistä. Kunnan tulee laatia suunnitelma niistä toimenpiteistä, joiden avulla organisaation tietoturvapolitiikka esitellään koko henkilökunnalle. Suunnitelmallista tietoturvaan liittyvää koulutusta tulee järjestää niin tietoturvasta vastaaville osastopäälliköille kuin koko kunnan henkilöstölle. Kunnan tulee olla mukana hankkeissa, joilla edistetään etätyön tekemistä ja sähköisen asioinnin kehittämistä.

Avainsanat: etätyö, standardi, sähköinen asiointi, tietoturva, tietoturvajohtaminen

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC

Master´s Degree Programme in Management of Technological Competence

Abstract of Master´s Thesis

Author	Keijo Ruonala	Year	2011
Commissioned by	Municipality in Northern Finland		
Subject of thesis	Information Security Management of a Municipality– Making Information Security a Part of Daily Routines of the Personnel		
Number of pages	58 + 1		

The topic of this thesis was to examine the level of information security in the researched area and to develop methods of making the procedures of information security part of the daily routines of the personnel. Other topics include the needs of developing telecommuting and e-services in the researched area.

The requirements and goals of the information security administration system and information security management are determined by the Information Security Standard SFS 27001(2006) and the municipality's own instructions concerning information security that are based on the Information Security Standard SFS 17799 (2005).

Information security management and the needs of developing telecommuting and e-services were examined by interviewing the heads of departments in the researched area. The research results were compared with the municipality's instructions and with the literature about the subject.

As the result of this research it was found out that the instructions concerning information safety meet the requirements of the standard SFS 27001. However, the instructions require regular updating. The municipality will have to make a plan of the measures of introducing the information security policy of the organization to the entire personnel. Systematic information security education must be arranged both for the heads of the departments responsible for the information security and for the whole municipality. The municipality will have to participate in projects promoting telecommuting and development of e-services.

Key words: telecommuting, standard, e-services, information security, information security management

SISÄLTÖ

KUVIOLUETTELO 1

1 JOHDANTO 2

1.1 Aiheen esittely 2
1.2 Tutkimuksen tavoite ja rajaus 4
1.3 Aihevalinnan perustelut 5
1.4 Työn eteneminen 5

2 TIETOTURVA KUNNALLISESSA ORGANISAATIOSSA 7

2.1 Lainsäädännöllinen tausta 7
2.2 Kunnan ja kuntakonsernin riskienhallinta 9
2.3 Riskienhallinta tietoturvajohtamisen näkökulmasta 10
2.4 Tietoturvajohtamisen käsitteitä 11
2.4.1 Luottamuksellisuus, eheys ja käytettävyys 11
2.4.2 Tietoturvallisuuteen liittyvät standardit 12
2.4.3 Tietoturvallisuuden hallinnoinnin toimintamallit 14
2.5 Tietoturvan osa-alueet 17
2.5.1 Tietoturvan osa-alueiden määrittely 17
2.5.2 Hallinnollinen turvallisuus 18
2.5.3 Fyysinen turvallisuus 19
2.5.4 Henkilöturvallisuus 21
2.5.5 Tietoaineistoturvallisuus 23
2.5.6 Ohjelmistoturvallisuus 24
2.5.7 Laitteistoturvallisuus 24
2.5.8 Tietoliikenneturvallisuus 25
2.6 Etätyö ja tietokoneen matkakäyttö 26
2.7. Sähköinen asiointi julkishallinnossa 27

3 TUTKIMUSMENETELMÄT JA AINEISTO 29

3.1 Tutkimusmenetelmät 29
3.2 Aineisto 30

4 TIETOTURVAKÄYTÄNNÖT TUTKIMUSKOHTEESSA 32

4.1 Tieturvapolitiikkaan liittyvät ohjeet tutkimuskohteessa 32
4.2 Käsitteen tietoturva ymmärtäminen 33
4.3 Haastateltavien tietoturvan eri osa-alueiden tuntemus 34
4.3.2 Fyysinen turvallisuus 34
4.3.3 Henkilöturvallisuus 34
4.3.4 Ohjelmistoturvallisuus 35
4.3.5 Laitteistoturvallisuus 36
4.3.7 Tietoaineistoturvallisuus 36
4.4 Hallinnollinen turvallisuus 37
4.4.1 Vastuu tietoturvapolitiikasta tutkimuskohteessa 37
4.4.2 Tietoturvapolitiikkaan liittyvien ohjeistojen tunteminen 38
4.4.3 Työnantajan järjestämä tietoturvaan liittyvä tiedotus ja koulutus 39
4.4.4 Tietoturvapoikkeaman käsittely tutkimuskohteessa 40
4.4.5 Toiminnan jatkuvuuden turvaaminen ongelmatilanteissa 41
4.4.5 Tietoturvallisuuden hallintajärjestelmän auditointi 42
4.5 Etätyö ja tietokoneen matkakäyttö 43
4.6 Sähköinen asiointi 44

5 JOHTOPÄÄTÖKSET 46

5.1 Toimenpide-ehdotukset 46
5.2 Pohdinta ja tutkimuksen luottavuuden arviointi 49

LÄHTEET 54

LIITTEET 58

KUVIOLUETTELO

Kuvio 1. Kunnan riskikartta 9
Kuvio 2. C.I.A -kolmikko 11
Kuvio 3. PDCA -malli 13
Kuvio 4. ITIL:n mukaiset tietoturvatoimenpiteet 15
Kuvio 4. Tietopääoman hallinta 23

Taulukko 1. GAISP:n toiminnalliset periaatteet 16
Taulukko 2. Laitteistoturvallisuus 21

1 JOHDANTO

1.1 Aiheen esittely

Tietoturvallisuus ja sen johtaminen on osa organisaation johdon tehtäväkokonaisuutta. Johdon on pystyttävä arvioimaan organisaation ja sen eri yksiköiden toiminnan aiheuttamat tietoturvavaatimukset. Tietoturvallisuuden johtamiseen on laadittu erilaisia viitekehyksiä, standardeja ja malleja. Tietoturva on otettava huomioon organisaation kaikissa yksiköissä osana päivittäistä johtamista. Tietoturva on saatava osaksi jokaisen työntekijän päivittäistä toimintaa. (Laaksonen–Nevasalo–Tomula 2006, 115.)

Tietoturvallisuudesta vain pieni osa hoidetaan tekniikan avulla. Suurin osa tietoturvallisuudesta hoidetaan henkilöstön tietoturvallisen käyttäytymisen avulla. (Puhakainen 2006; Koskivirta 2006.)

Tutkittava kunta on toteuttanut yhdessä konsulttiyrityksen kanssa tietoturvan hallinnan koulutus- ja kehittämisprosessin vuosina 2006–2007. Hankkeen tavoitteena oli nostaa henkilöstön tietoturvan hallinnan tasoa, tehdä laaja-alainen tietoturvakartoitus ja toteuttaa koko kunnan organisaatiota koskeva tietoturvan hallinnan järjestelmä. (Kohdekunta 2007b.)

Kehittämishankkeessa toteutettiin tietoturvakartoitus, joka dokumentoitiin yksityiskohtaisesti. Hankkeen aikana laadittiin ohjeet tietojärjestelmien hallinnointiin, tietojen ja asiakirjojen luokitteluun, tietoturvaan, tietosuojaan, tietoturvapoikkeamien käsittelyyn ja etätyöhön. Tietoturvapolitiikka sekä tietoturva- ja tietosuojaohjeet esiteltiin henkilöstölle järjestetyssä koulutuksessa vuonna 2006. (Kohdekunta 2007b.)

Tutkimuskohteessa kunnanhallitus vastaa kunnan tietoturvapolitiikasta. Kunnanhallitus ja kunnan johto määrittävät tietoturvapolitiikan avulla tietoturvallisuuden tavoitteet, vastuut ja toteutuskeinot. Vastuunjaon mukaisesti kunnan ATK-osasto vastaa ATK-päällikön johdolla järjestelmien ylläpidosta ja tietoturvallisuuteen liittyvistä ehdotuksista sekä niiden toteuttamisesta. Osastopäälliköt vastaavat osastojensa tietoturvatoimenpiteiden toimeenpanosta ja

organisoinnista. Kunnan henkilökunta on velvoitettu toimimaan tietoturvapolitiikan ja siitä annettujen ohjeiden mukaan. (Kohdekunta 2007d.)

Suomen kuntaliiton tekemän selvityksen mukaan teknisesti ja juridisesti etätyöhön on mahdollisuus noin 41 prosentilla selvitykseen osallistuneista kuntien työntekijöistä ja 40 prosentilla kentällä liikkuvaa työtä tekevistä oli mahdollisuus käyttää tarvitsemiaan tietojärjestelmiä etäyhteydellä. (Kettunen 2010, 6.)

Etätyöllä tarkoitetaan työnteon muotoa, jossa työ tehdään joko osin tai kokonaan kotona tai muussa työntekijän valitsemassa paikassa ja se nähdään yhteä keinona nykyaikaistaa työn organisointia ja sovittaa yhteen työ- ja vapaa-aika. Etätyön avulla halutaan parantaa työn tuottavuutta ja työelämän laatua. Työssä jaksaminen, työn ja perhe-elämän yhteensovittaminen, työ- ja asuinpaikan joustava sijoittuminen ovat myös merkittäviä etuja puhuttaessa etätyöstä. Etätyön tekeminen vähentää matkakustannuksia ja siihen käytettävää aikaa. (Työ- ja elinkeinoministeriö 2010; Kuntatyönantajat 2010.)

Tutkimuskohteessa etätyön tekeminen hyödyntäen informaatioteknologian tarjoamia mahdollisuuksia ei ole toistaiseksi mahdollista, koska etäyhteys yksittäisestä verkon ulkopuolisesta työasemasta ei ole sallittua kunnan verkkoon. (Kohdekunta 2007c.)

Sähköinen asiointi on lisääntynyt Suomen kunnissa. Verkon kautta voi hoitaa yhä useampia asioita. Kirjastot ovat olleet etunenässä kehittämässä sähköisiä palveluitaan. Lisäksi monet lomakkeet ja tilojen varaukset ovat tarjolla verkossa. Sähköisen asioinnin uskotaan lisäävän kuntalaisten tyytyväisyyttä kunnallisiin palveluihin. (HighTech Forum Oulu 2007.)

Laki sähköisestä asioinnista viranomaistoiminnassa on tullut voimaan vuonna 2003. Lain tavoitteena on, että viranomaistoiminnassa voitaisiin siirtyä laajalti käyttämään sähköistä asiointia. Sähköistä asiointia viranomaistoiminnassa koskevan lain 2 luvun 5 §:n mukainen kuntien velvollisuus tarjota mahdollisuus sähköiseen asian vireille saattamiseen koskee vain niitä kuntia, joilla on tarvittavat tekniset, taloudelliset ja muut valmiudet vireillepanon toteuttamiseen. (Laki sähköisestä asioinnista viranomaistoiminnassa 2003.)

1.2 Tutkimuksen tavoite ja rajaus

Kunnan johto halusi selvittää opinnäytetyöni avulla tietoturvapolitiikan käytännön toteutumista kunnan organisaatiossa. Opinnäytetyön näkökulmaksi valittiin tietoturvajohtaminen, jolla käytännössä eniten vaikutetaan henkilöstön tietoturvalliseen käyttäytymiseen. Tämän lisäksi haluttiin selvittää myös etätyöhön ja sähköiseen asiointiin kohdistuvat kehittämistarpeet ja -toiveet. Tutkimuksen keskeisiä tuloksia peilataan kunnan omiin ohjeisiin ja alan muihin auktoriteetteihin. Tulosten perusteella laaditaan esitykset niistä toimenpiteistä, joilla tietoturvajohtamista ja tietoturvan jalkauttamista henkilöstön pariin voidaan parantaa. Etätyön ja sähköisen asioinnin kehittämistarpeet kirjataan tutkimustulosten perusteella.

Tutkimus toteutettiin laadullisena tutkimuksena. Tutkimukseen haastateltaviksi valittiin tutkittavan kohteen osastopäälliköt hallinto-osastolta, perusturvasta, sivistystoimesta ja tekniseltä osastolta. Osastopäälliköt vastaavat tietoturvapolitiikan vastuunjaon perusteella käytännön toimista tietoturvapolitiikan toteutumiseksi. Haastattelun tavoitteena oli selvittää osastopäälliköiden yleinen tietämys tietoturvasta ja sen eri osa-alueista. Haastattelun avulla selvitettiin myös haastateltavien tapa toimia tietoturvajohtajina ja tietoturvajohtamiseen liittyvät kehittämistarpeet. Etätyö ja sähköinen asiointi ja etenkin niiden kehittäminen olivat yhtenä haastatteluteemana.

Tutkimuskysymyksinä olivat:

1. Mikä oli haastateltavien yleinen tietämys tietoturvasta ja sen osa-alueista?
2. Miten haastateltavat toimivat tietoturvajohtajina ja mitkä olivat tietoturvajohtamiseen liittyvät kehittämistarpeet?
3. Mitä kehittämistarpeita haastateltavilla oli etätyöhön ja sähköiseen asiointiin liittyen?

Teemahaastattelun (liite 1.) kysymykset pohjautuivat tutkimuskysymyksiin ja tietoturvastandardiin SFS 27001. Pääteemojen tueksi on laadittu joukko tarkentavia kysymyksiä, joita esitin haastateltaville.

1.3 Aihevalinnan perustelut

Tutkimusaiheen valinta perustuu pitkään kokemukseeni kunnallisista luottamustoimista. Olen ollut kunnallisissa luottamuselimissä viitenä eri valtuustokautena. Luottamustoimissani olen havainnut, että riskienhallinta ja siinä yhtenä osana mukana oleva tietoturvan hallinta ja tietoturvajohtaminen ovat nousseet tärkeään osaan sekä operatiivista että poliittista johtamista.

Toisena aiheen valintaan vaikuttava tekijänä on oma koulutukseni ja työkokemukseni. Olen koulutukseltani insinööri (amk), sähkötekniikan koulutusohjelmasta. Opiskeluni suuntautuivat tietotekniikkaan, jossa yhtenä tärkeänä osa-alueena olivat tietoturvaan liittyvät kysymykset. Työskentelen tällä hetkellä opettajana toisen asteen ammatillisessa oppilaitoksessa. Työssäni joudun tekemisiin tietoturvakysymysten kanssa, varsinkin tietoturvaan liittyvän lainsäädännön kanssa, joka on esitelty luvussa 2.1. Olen ollut myös eri työpaikoissa, joissa tietoturvaan liittyvät seikat ovat liiketoiminnan jatkuvuuden kannalta keskeisiä. Näistä työpaikoista voisin mainita suomalaisen ohjelmistotalon, jossa työskentelin vuosina 1999–2000.

Kolmas ja ratkaiseva tekijä aiheen valintaan oli tutkimuskohteen virkamiesjohdon tarve selvittää tietoturvajohtamiseen ja tietoturvapolitiikan jalkauttamiseen liittyviä kysymyksiä. He olivat havainneet, että pelkästään hyvät ja sinänsä ajantasaiset tietoturvapolitiikkaan liittyvät ohjeet eivät takaa organisaation tietoturvallista toimintaa.

1.4 Työn eteneminen

Tutkimustyön ensimmäisessä vaiheessa perehdyin tietoturvallisuuden standardeihin, alan kirjallisuuteen ja tutkimuskohteen tietoturvapolitiikkaan. Tämä vaihe on tosin jatkunut läpi koko päättötyöprosessin. Tutkimuksen toteuttaminen on vaatinut myös teemahaastattelusta kertovaan kirjallisuuteen perehtymistä. Ajallisesti kyseessä on kevät 2010 – kevät 2011.

Tutkimusmenetelmäksi valitsin laadullisen tutkimuksen. Teemahaastattelut toteutettiin keväällä 2010. Tutkimusaineistot ja menetelmät on esitetty luvus-

sa 3 samoin kuin tarkempi kuvaus tutkimuksen etenemisestä. Tutkimuksen vaiheita on peilattu samalla alan auktoriteettien kirjallisuuteen.

Tutkimuksen raportointi on ajoittunut keväälle 2011. Tutkimuksen tulokset on esitelty luvussa 4 ja johtopäätökset sekä toimenpide-ehdotukset on esitelty luvussa 5.

2 TIETOTURVA KUNNALLISESSA ORGANISAATIOSSA

2.1 Lainsäädännöllinen tausta

Suomen lainsäädännöstä ei löydy varsinaista tietoturvalakia. Tietoturvaan liittyviä asioita käsitellään useiden eri lakien ja määräysten yhteydessä. Seuraavassa on esitetty kaksi keskeistä periaatetta, jotka vaikuttavat kuntien harjoittamaan tietoturvapolitiikkaan. Nämä periaatteet on määritelty Laissa viranomaisten toiminnan julkisuudesta ja Henkilötietolaissa. (Valtionvarainministeriö 2011.)

> *Viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä."* (Laki viranomaisen toiminnasta julkisuudessa 1999.)

> *Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä*." (Henkilötietolaki 1999.)

Tietoturvallisuus pohjautuu viranomaistoiminnan julkisuudesta annetun lain ja asetuksen lisäksi moniin muihin eri lakeihin. Mm. perustuslaki määrää, että yksityiselämän suoja ja julkisuusperiaate ovat kansalaisten perusoikeuksia. Erilaisten lakeihin sisältyvien salassapitosäännösten lisäksi tärkeimpiä tietoturvaan vaikuttavia lakeja ovat Laaksosen, Nevasalon ja Tomulan (2006, 27–32) sekä Valtiovarainministeriön (2011) Tietoturvaoppaan mukaan:

− Perustuslaki (1999) 2.luku 10 § (Yksityiselämän suoja ja luottamuksellisen viestin salaisuus)

− Perustuslaki (1999) 2.luku 12 § (Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus)

− Laki viranomaisten toiminnan julkisuudesta (1999)

− Henkilötietolaki (1999) (Henkilötietojen käsittelyä koskevat yleiset periaatteet)

− Arkistolaki (1994) (Asiakirjojen laatiminen, säilyttäminen ja käyttö)

− Valtion virkamieslaki (1994) 17§ (Säädös valtion virkasuhteesta)

− Laki kunnallisesta viranhaltijasta (2003)

− Työsopimuslaki (2001)

− Rikoslaki (1889) 34.luku 9a § (Vaaran aiheuttaminen tietojenkäsittelylle)

− Rikoslaki (1889) 38.luku 8 § (Tietomurto)

− Rikoslaki (1889) 38.luku 9 § 1. kohta (Henkilötietorikos)

− Henkilötietolaki (1999) 48 § (Henkilörekisteririkkomus)

− Vahingonkorvauslaki (1974)

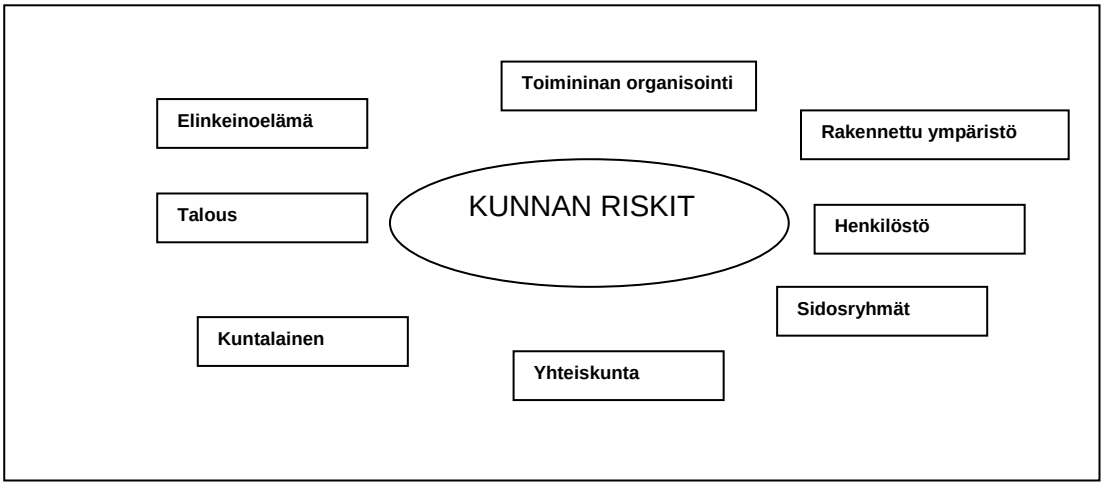
− Laki yksityisyyden suojasta työelämässä (2001)

- Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (1999).

2.2 Kunnan ja kuntakonsernin riskienhallinta

Kunnan tietoturvapolitiikan lähtökohtana on riskianalyysi, jonka avulla olemassa olevat uhat saadaan paikallistettua, vaiheen perusteella luodaan ohjeistus ja toimintaohjeet. Hallinnollisessa tietoturvassa päämääränä on luoda organisaatioon toimintatapa, jolla pystytään välttämään tietoturvariskit. (VirtuaaliAMK 2011.)

Riskienhallinta on johtamisen väline, joka keskittyy organisaation riskeihin. Riskienhallinnan tavoitteena on järjestelmällisesti vähentää erilaisten riskien aiheuttamia haittavaikutuksia ja kustannuksia. Kuviossa 1 kuvataan, miten riskienhallinnan tulee kattaa kaikki kunnan toimintaan liittyvät riskin ja ongelma-alueet. Riskienhallinnan avulla pyritään kunnan toiminnan jatkuvuuden turvaamiseen tilanteessa, joissa jokin tai jotkin riskit realisoituvat. (Enberg 2002, 12; Kuntaliitto 2011a, 5.)



Kuvio 1. Kunnan riskikartta (mukaillen Kuntaliitto a. 2011, 5)

Kuntakonsernin tytäryhtiöissä ja tytäryhteisöissä voidaan noudattaa yhtenäisiä toimintaperiaatteita. Riskienhallintaohjelman asettamat velvoitteet voidaan ulottaa koskemaan koko kuntakonsernia. Kunnan toimielimet ja vastuuhenkilöt konsultoivat ja koordinoivat konserniyhteisöjen riskikartoituksen tekemistä ja antavat määräyksiä toimivaltansa puitteissa riskienhallintaan liittyvissä asioissa. (Kuntaliitto 2011b, 20.)

Hyvä ja tehokas tietoturvajohtaminen sisältää aina huolellisen riskianalyysin (Pfleeger–Pfleeger 2003, 506). Riskianalyysin lähtökohtana tulee olla organisaation kokonaisturvallisuus. Riskianalyysi voidaan jakaa kahteen osaan, riskikartoitukseen ja riskien arviointiin. Riskikartoituksen avulla haetaan toimintaan liittyvät riskit ja uhkakuvat. Kartoituksen tulee olla systemaattista. Löydettyjen riskien ja uhkakuvien vaikutusta organisaation toimintaan arvioidaan sopivilla mittareilla, joiden avulla on tarkoitus selvittää, kuinka vakavia vahinkoja eheys-, käytettävyys- ja luottamuksellisuusriskit voivat organisaatiolle aiheuttaa. (Hakala–Vainio–Vuorinen 2006, 79–82.)

2.3 Riskienhallinta tietoturvajohtamisen näkökulmasta

Tietoturvallisuuden tärkein osa on riskienhallinta. Riskienhallinnan avulla pyritään näkemään tulevaisuuteen ja näin pienentämään yritykseen (kuntaan) vaikuttavien uhkien toteutumismahdollisuus. Toisaalta riskienhallinnan avulla voidaan havaita ja hallita yrityksen toimintaan kohdistuvia ei-toivottuja tapahtumia. Kaikkia riskejä ei voi kokonaan poistaa, niinpä riskienhallinnalla pyritään riskien pienentämiseen hyväksyttävälle tasolle. Testaamalla tietoturvaa havaitaan tietoturvaheikkoudet, suojaustoimenpiteiden toimivuus sekä mahdolliset puutteet toiminnassa. (Krutz–Vines 2003, 16; Laaksonen ym. 2006, 150.)

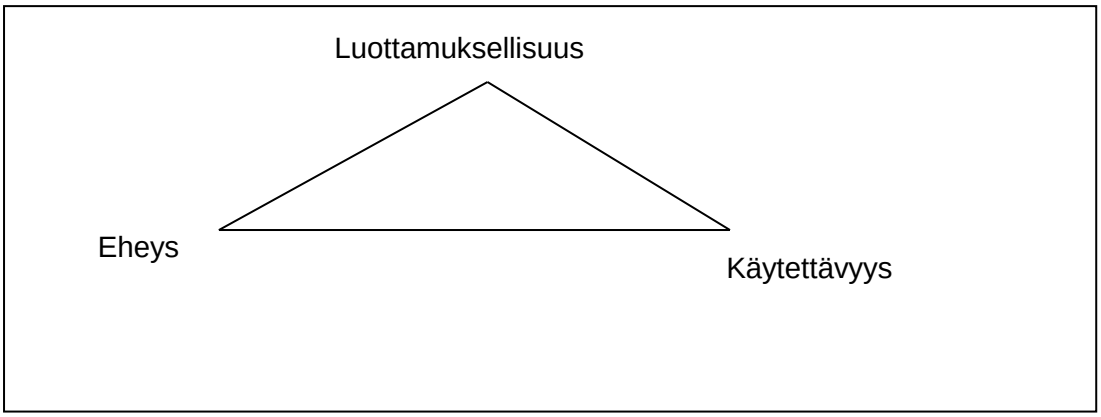
Tietoturvallisuusstandardi ISO 27001 mukaan yrityksellä tulee olla yhteisesti sovittu tapa arvioida riskejä sekä yhdessä sovittu menetelmä tietoturvallisuuden testaamiseksi. Riskien arviointi tulee ulottaa myös ulkoistettuihin palveluihin, kuntatasolla tytäryhtiöihin ja -yhteisöihin. Säännöllisyys ja aikataulutus tekevät riskien arvioinnista tehokasta. Arviointien ja analyysien pitää johtaa myös toimintaan, mikäli tarvetta ilmenee. (SFS 27001 2006b.)

Riskikartoituksista ja tietoturvaan liittyvistä testaustuloksista tulee raportoida toimivalle johdolle ja myös muille tahoille, joita ne koskettavat. Kuntaorganisaatiossa tietoturvasta vastaavana tahona on useimmiten kunnanhallitus. Kunnanhallituksen esittelijänä toimii kunnanjohtaja. (Laaksonen ym. 2006, 150.)

2.4 Tietoturvajohtamisen käsitteitä

2.4.1 Luottamuksellisuus, eheys ja käytettävyys

Tietoturvallisuuden kolme keskeistä käsitettä ovat luottamuksellisuus, eheys ja käytettävyys (C.I.A., Confidentiality, Integrity, Availability). Tietoturvallisuuteen liittyvät turva- ja valvontamekanismit, uhat, heikkoudet ja prosessit liittyvät C.I.A:han. (Krutz–Vines 2003, 3; Pfleeger–Pfleeger 2003, 9–12.)



Kuvio 2. C.I.A. -kolmikko (mukaillen Krutz–Vines 2003, 3)

Luottamuksellisuudella tarkoitetaan sanoman sisällön paljastumisen estämistä. Paljastuminen voi olla tahallista tai tahatonta. Luottamuksellisuuden menettäminen voi tapahtua esimerkiksi verkon käyttöoikeuksien väärinkäytön seurauksena. Toinen tapa menettää luottamuksellisuus on tahattomasti tapahtuva yrityksen/kunnan tietojen luovuttaminen vääriin käsiin. (Krutz–Vines 2003, 3; Pfleeger–Pfleeger 2003, 10.)

Eheydellä varmistetaan, etteivät prosessit tai valtuuttamattomat henkilöt muuta käsiteltäviä tietoja. Toisaalta pyritään varmistumaan siitä, että valtuutetut henkilöt tai prosessit tekevät niille myönnettyjä valtuuksia käyttäen luvallisia muutoksia tietoihin. Kolmas eheydelle asetettu vaatimus on se, että tiedot ovat yhdenmukaisia niin sisäisesti kuin ulkoisesti tarkasteltuina. (Krutz–Vines 2003, 3; Pfleeger–Pfleeger 2003, 10–11.)

Käytettävyydellä taataan se, että tiedot ja resurssit sekä turvapalvelut ovat aina niitä tarvitsevien käytettävissä. Käytettävyys takaa myös järjestelmien toimivuuden. (Krutz–Vines 2003, 3; Pfleeger–Pfleeger 2003, 11–12.)

2.4.2 Tietoturvallisuuteen liittyvät standardit

Laaksonen, ym. (2006) esittää tietoturvaan ja tietoturvajohtamisen liittyvät standardit.

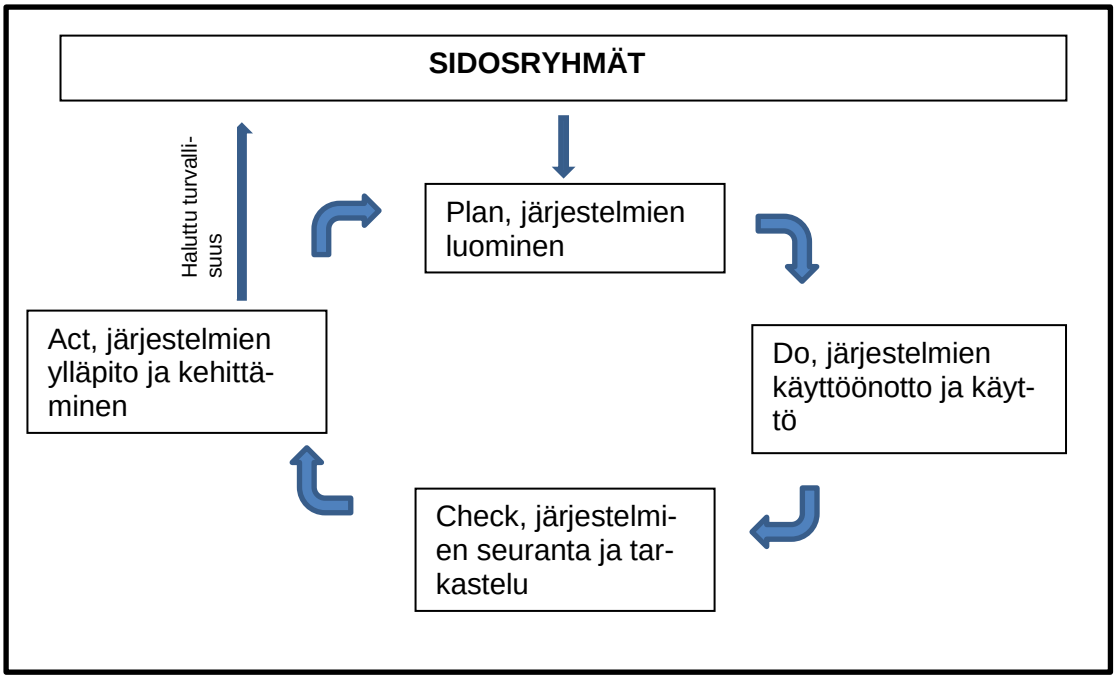
ISO -standardit ovat keskeisimpiä tietoturvastandardeja. Ne ovat laajasti tunnustettuja standardeja, jotka ovat pääsääntöisesti suunniteltu yksityisen sektorin käyttöön. ISO -standardit soveltuvat kuitenkin hyvin myös julkiselle sektorilla käytettäviksi. Tärkeimpiä ISO -standardeja ovat:

ISO 17799 -standardin avulla ja sen suosituksia noudattamalla voidaan varmistua siitä, että tietoturvallisuuden kannalta keskeiset asiat tulevat otetuksi riittävässä laajuudessa huomioon. Tämä vuonna 2005 julkaistu standardi pohjautuu **BS 7799** -standardiin vuodelta 1995**.**

ISO 27000 -standardisarjassa määritellään yleiset vaatimukset tietoturvallisuuden hallintajärjestelmän luomiselle, toteuttamiselle, käyttämisellä, valvonnalle, katselmoinnille, ylläpidolle ja parantamiselle. Standardissa esitetyt yleiset vaatimukset ovat sovellettavissa organisaation tyypistä, koosta tai luonteesta riippumatta. (ISO 27000 Directory 2009.)

ISO 27001 -standardi vuodelta 2005 määrittelee ne tietoturvallisuuden hallintajärjestelmälle asetettavat vaatimukset, jotka mahdollistavat riskien arvioinnin ja toimenpiteet joilla ehkäistään riskien toteutuminen. Tähän standardiin perustuvan tietoturvallisuuden hallintajärjestelmän avulla saadaan yrityksen/kunnan tietovarannot pidettyinä luottamuksellisina, ehyinä ja saatavilla. Samalla suojataan tietoja häviämiseltä tai joutumiselta vääriin käsiin. Standardia noudattamalla tunnistetaan organisaation kohdistuvat tietoturvauhat. Standardin mukaisen toiminnan avulla johto saa työkalun toiminnan ohjaukselle ja samalla se voi osoittaa sidosryhmilleen, että organisaatiolla on tietoturvallisuuteen liittyvät asiat hallinnassaan. (ISO 27001 Sertifiointi 2011.)

ISO 27001 standardin perusajatuksena on kuviossa 3 esitetty tietoturvallisuuden hallintajärjestelmän prosessinomainen kehittäminen PDCA -mallin mukaisesti. PDCA on lyhenne sanoista plan, do, check ja act.



Kuvio 3. PDCA -malli (mukaillen Hakala ym. 2006, 49)

Tietoturvallisuuden hallintajärjestelmiä käsittelevään kansainväliseen standardiin ISO 17799:2005 on julkaistu tekninen korjaus. Standardin tunnus on muutettu muotoon **ISO 27002:2005**. Standardi on julkaistu suomeksi tunnuksella ISO 17799:fi, eikä suomennoksen tunnusta ole muutettu. Julkaisu on saanut suomenkieliseksi nimekseen; Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. (SFS 27002 2007.)

ISO 27005 -standardi vuodelta 2008 kuvaa tietoturvallisuuden riskienhallintajärjestelmän, joka koostuu hallinnan yhteyden määrittelystä, riskiarvioinnista, riskien käsittelystä, riskien hyväksynnästä, riskien tiedottamisesta, riskien seurannasta ja katselmoinnista. Standardin tarkoituksena on edesauttaa stadardien ISO 27001 ja ISO 27002 soveltamista ja käyttöönottoa. (Yhteiskunnan Tieto – Knowledge of Society 2008.)

Tietoturvastandardit on kehitetty tietoturvasuunnittelun jäsentämistä ja organisointia varten. Ne eivät aseta vaatimuksia tietoturvan tasolle ja sisällölle. Suurin hyöty standardeista saadaan tietoturvan dokumentoinnissa, koska ne tarjoavat selkeän ja vertailukelpoisen rakenteen syntyneille dokumenteille.

Standardien tehtävänä on ainoastaan määritellä, mitä suunnittelutyö sisältää ja missä muodossa sen tulokset esitetään. Standardien noudattaminen ei yksin takaa riittävän tasoista tietoturvallisuutta. (Hakala ym. 2006, 46.)

2.4.3 Tietoturvallisuuden hallinnoinnin toimintamallit

Tietoturvallisuuden hallinnointiin on kehitetty useita eri malleja, joista osa käsittelee ainoastaan tietoturvallisuutta ja osa keskittyy liiketoiminnan kokonaisuuden tukemiseen. Malleissa esitetään tietoturvallisuuden kannalta keskeisiä osa-alueita, prosesseja ja kontrolleja. (Laaksonen ym. 2006, 91.)

Laajalle levinneitä standardeja ja malleja hyödyntävät organisaatiot ja tietoturvallisuudesta vastaavat henkilöt voivat olla suhteellisen varmoja siitä, että mikään tietoturvallisuuden kannalta oleellinen osa-alue ei ole jäänyt huomioimatta suunnittelussa (Laaksonen ym. 2006, 104).

COBIT (Control Objectives for Information and related Technology) on viitekehys, jonka avulla organisaatio voi määritellä tietojenkäsittelyn liiketoiminnallisia tavoitteita ja vaatimuksia. COBIT auttaa organisaation johtoa yhdistämään liiketoiminnan ja IT-toimintojen tavoitteet sekä antaa mittarit, joilla tavoitteiden saavuttamista voi seurata. COBIT on teknologiasta riippumaton viitekehys, joka ei ota kantaa siihen, miten asiat käytännössä täytyy hoitaa. COBIT auttaa tunnistamaan ja määrittelemään monia tietoturvallisuuden kannalta keskeisiä prosesseja. Viitekehyksen on kehittänyt ISACA (Information System Audit and Control Associations). (Laaksonen ym. 2006, 92–95.)

ITIL (Information Technology Infrastructure Library) on kokoelma parhaista käytännöistä, jotka liittyvät tietojenkäsittelyn palvelutuotantoon. ITIL on vapaasti käytettävissä ja se onkin laajasti käytössä tietotekniikan palveluyritysten palvelujen standardoinnin viitekehyksenä. ITIL tarjoaa mallin tietojärjestelmien ja tietohallinnon toimintojen tehokkuuden mittaamiseen. ITIL sisältää neljän P:n mallin, joka käsittää ihmiset (People), toimintaprosessit (Processes), IT-palveluissa käytettävät tuotteet, työkalut ja teknologian (Products) ja

sidosryhmät (Partners). Organisaation johdon yhdistää nämä neljä aluetta toisiinsa toimivalla ja tehokkaalla tavalla. ITIL korostaa palvelujen laatua. Palvelujen laatua voidaan parantaa kuuntelemalla asiakkaan tarpeita ja vaatimuksia sekä varmistamalla, että ne täyttyvät palveluiden eri vaiheissa. ITIL sopii kaiken kokoisille yrityksille ja se koostuu seitsemästä osasta, jotka ovat:

- IT-palvelujen tuottaminen
- IT-palvelujen tuki
- IT-palvelujen suunnittelu
- Turvallisuuden hallinta
- Infrastruktuurin hallinta
- IT-toimintojen liiketoiminnallinen näkökulma
- Sovellusten hallinta.

ITIL määrittelee tietoturvallisuuden johtamisen periaatteet, joissa otetaan huomioon tietoturvallisuus jo palvelujen suunnitteluvaiheessa. Tietoturvallisuuden johtamisen avulla varmistutaan siitä, että organisaatiolla on riittävä määrä kontrolleja, joilla ehkäistään uhkatilanteita. Kontrollien avulla havaitaan vaaratilanteet ja korjataan aiheutuneet vahingot. ITIL edellyttää tietoturvan säännöllistä tarkastamista ja raportointia tietoturvallisuuden nykytilasta ja näin ollen sen perusajatus ei poikkea standardin SFS 27001 vaatimuksista. Kuviossa 4 kuvataan ITIL:n mukaiset organisaation tietoturvatoimenpiteet (Laaksonen ym. 2006, 95–99.)

Kuvio 4. ITIL:n mukaiset tietoturvatoimenpiteet (mukaillen Laaksonen ym. 2006, 99)

GAISP (Generally Accepted Information Security Principles) on kattava viitekehys riippumatta siitä, mitä periaatteita, standardeja tai menetelmiä tietoturvatyössä käytetään. Viitekehyksessä on neljätoista yleisluonteista toiminnallista periaatetta operatiiviselle johdolle sovellettavaksi. (Laaksonen ym 2006, 100). Periaatteet esitellään sivulla 16 olevassa tauloukossa.

Taulukko 1. GAISP:n toiminnalliset periaatteet (mukaillen Laaksonen ym. 2006, 101–103).

Tietoturvapolitiikka	Johdon tulee varmistua, että tietoturvapolitiikka ja sitä tukevat standardit, parhaat käytännöt ja minimivaatimukset kattavat tietoturvallisuuden kaikki osa-alueet.
Koulutus ja tietoisuuden lisääminen	Varmistuakseen tietoturvatavoitteiden ymmärtämisestä, johdon tulee säännöllisesti keskustella henkilöstön kanssa tietoturvatavoitteista. Koulutuksen tulee sisältää riittävässä määrin teoria, joka selittää käytännön ohjeistusta ja toimintatapoja.
Jäljitettävyys	Johdon tulee määritellä tarkasti, mitä työntekijät saavat tehdä. Oikeudet tiedon muokkaamiseen, kopiointiin ja tuhoamiseen tulee rajata siten, että vain nimetyllä käyttäjällä on oikeus tarpeellisiin toimiin.
Tiedonhallinta	Organisaation toiminnan kannalta oleellinen tieto tulee määritellä. Tiedolle tulee antaa arvo ja se tulee luokitella. Tiedon määrittelyssä tulee ottaa huomioon tiedon luotettavuus ja eheys.
Ympäristön hallinta	Tietoturvan suunnittelussa tulee huomioida ympäristö ja siitä aiheutuvat luonnolliset riskit kuten tulipalot.
Työntekijöiden osaaminen	Työntekijöille tulee antaa oikeuksia tietojenkäsittelyyn heidän osaamisena ja työtehtävän mukaisesti.
Virhetilanteiden hallinta	Organisaatiolla on oltava selvät toimintatavat virhetilanteiden varalta.
Tietojärjestelmien elinkaari	Tietoturvallisuus tulee huomioida tietojärjestelmien koko elinkaaren aikana.
Pääsynvalvonta	Pääsyoikeudet tietoon saa olla vain niillä, jotka tarvitsevat tietoa työnteossaan. Johdon on laadittava riittävät kontrollit, jotta tästä voidaan varmistua.
Jatkuvuussuunnittelu	Tietojärjestelmien pitkäaikaisten keskeytymisien varalle laaditaan ajantasainen jatkuvuussuunnitelma.
Riskienhallinta	Johdon tulee varmistua siitä, että tietoturva on linjassa arvioitujen riskien kanssa.
Tietoliikenteen turvallisuus	Johdon tulee olla tietoinen tietoliikenteeseen liittyvistä riskeistä.
Lain- ja vaatimustenmukaisuus	Johdon tulee olla jatkuvasti selvillä lakien ja muiden tahojen asettamista vaatimuksista.
Eettinen toiminta	Johdon tulee ottaa huomioon yksityisyydensuoja ja eettiset periaatteet tietoturvapolitiikkaa suunniteltaessa.

Hakala, Vainio ja Vuorinen (2006, 106–113) esittelevät kirjassaan tietoturvallisuuden hallintajärjestelmän, joka pohjautuu tietoturvastandardiin SFS 27001. Hallintajärjestelmän nimi on **ISMS** (Information Security Managemet System). Tässä mallissa tieturvajohtaminen ja tietoturvallisuuden hallinta nähdään prosessina jossa, järjestelmää kehitetään koko ajan vastaamaan organisaation toiminnan muutosten ja toimintaympäristön muutosten aiheuttamiin turvallisuustarpeisiin. ISMS -järjestelmän luominen aloitetaan tekemällä määritys ja kuvaus niistä asioista, jotka kuuluvat järjestelmään. Kuvauksessa on otettava huomioon organisaation toimiala ja liiketoiminta, organisaatiorakenne, toimipaikat, aineellinen ja aineeton omaisuus, käytössä olevat tekniikat ja ulkopuolelle rajatut toiminnot tai tietojärjestelmät perusteluineen. ISMS -järjestelmässä käsitellään ne käytännöt, joiden avulla turvallisuutta hallitaan. Järjestelmällä tulee olla organisaation johdon hyväksyntä ja tuki. ISMS -järjestelmässä luodaan riskienhallintamekanismit, jotka jaetaan eri osa-alueisiin. Osa-alueet ovat käytäntöön soveltuvien riskiarviointimenetelmien määrittely, riskien tunnistaminen, riskien analysointi ja vaikutusten arviointi, riskien käsittelyyn liittyvien vaihtoehtojen määritys ja arviointi, tavoitteiden asettaminen ja kontrollien valinta sekä jäännösriskien hyväksyttäminen. Tietoturvallisuuden hallintajärjestelmä vaatii lisäksi runsaasti eritasoista dokumentointia. Dokumentit voivat olla asiakirjamuotoisia tai ne tallennetaan lokitiedostoihin ja hallintasovellusten tietokantoihin.

2.5 Tietoturvan osa-alueet

2.5.1 Tietoturvan osa-alueiden määrittely

Tietoturva on erittäin laaja kokonaisuus ja se halutaan usein jakaa pienempiin osiin. Näin siitä saadaan helpommin käsiteltäviä osia. Samalla näistä osa-alueista laadittavista dokumenteista saadaan rakenteeltaan selkeämpiä. Hakala, Vuorinen ja Vainio (2006, 10) kuvaavat tietoturvan osa-alueet seuraavasti:

- hallinnollinen turvallisuus
- fyysinen turvallisuus
- henkilöturvallisuus
- tietoaineistoturvallisuus
- ohjelmistoturvallisuus
- laitteistoturvallisuus
- tietoliikenneturvallisuus.

Tietoturvan osa-alueet on määritelty monella eri tavalla. Viestintävirasto (2009) määrittelee ne seuraavasti:

- hallinnollinen ja organisatorinen tietoturvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- käyttöturvallisuus.

Tässä mallissa tietoturvallisuuden osa-alueet on jaettu kahdeksaan alueeseen, joiden perusteella käyttäjät ja organisaatio toteuttavat tietoturvaan liittyvät tehtävät, kuten suunnittelun ja valvonnan. (Viestintävirasto 2009.)

Seuraavassa käsitellään tietoturvan osa-alueita yksityiskohtaisemmin Tietoturvallisuuden käsikirjan (Hakala ym. 2006, 10) jaottelun mukaisesti.

2.5.2 Hallinnollinen turvallisuus

Hallinnollinen turvallisuus liittyy tietoturvan kehittämiseen ja johtamiseen pitäen sisällään yhteydenpidon eri viranomaisiin ja toimielimiin, jotka vastaavat tietoturvallisuudesta organisaation sisällä sekä sen ulkopuolella. Toiminnan keskiössä ovat lainsäädännön ja erilaisten lisenssisopimusten ja palvelusopimusten vaikutusten arviointi tietoturvassa käytettävien menetelmiin. Hallinnollisesta turvallisuudesta vastaa yleensä organisaation tietohallinto. (Hakala ym. 2006, 10–11; SFS 27001 2006, 32–33.)

Tietoturvan hallintajärjestelmän toteuttaminen ja käyttäminen kuvataan standardissa SFS 27001.

Hallinnollinen tietoturvallisuus on keskeinen osa tietoturvallisuuden johtamistoimintoa ja se muodostaa lähtökohdan organisaation koko tietoturvatoiminnalle. Se muodostuu periaatteista, jonka organisaation johto on hyväksynyt. Kunnallisessa organisaatiossa kyseessä on johtosäännön mukainen päätöksentekojärjestys. Hallinnollisessa tietoturvassa on kysymys myös vastuunjaosta, resurssien varaamisesta sekä riskien arvioinnista. Hallinnollisen tieto-

turvan avulla luodaan organisaatiolle tietoturvalliset toimintatavat ja toimintamallit. Toimintamallien pohjalta luodaan henkilöstön koulutusjärjestelmät liittyen tietoturvaan sekä välttämättömät ohjeistukset sekä valvonta- ja tarkastusmenettelyohjeet tietoturvan ylläpitämiseksi ja kehittämiseksi. (SFS 27001 2006, 14–20.)

Hallinnollisessa turvallisuudessa on oleellista, että käyttäjät tietävät ja ymmärtävät ne periaatteet, joille organisaation tietoturvallisuus rakentuu. Tätä varten organisaation johdon tulee julkaista organisaation tietoturvapolitiikka. Politiikka jaetaan koko henkilökunnalle. Tietoturvapolitiikan tueksi tulee suunnitella organisaation ohjekokonaisuus ja määritellä vaadittu tietoturvakuvausten taso. Lisäksi laaditaan tietoturvasuunnitelmat, jotka osoittavat organisaatiolle elintärkeät tietojärjestelmät, niiden toipumistoimet sekä vaatimukset poikkeusolojen valmiudelle. (SFS 27001 2006, 14–20.)

Tietoturvallisuuden hallintajärjestelmän sisäiset ja ulkoiset auditoinnit ovat keskeinen osa hallinnollista tietoturvaa. Organisaation tulee suunnitella ja suorittaa tietyin aikavälein tietoturvallisuuden auditointeja selvittääkseen, ovatko tietoturvallisuuden hallintajärjestelmän velvoitteet, eri turvamekanismit, prosessit ja menettelytavat suunnitelmien ja standardin SFS 27001 mukaisia ja lainsäädännön mukaisia. Lisäksi selvitetään onko toiminta ollut tunnustettujen tietoturvavaatimusten mukaista, vakuuttavasti toteutettua ja ylläpidettyä. Menettelytapaohje, joka on dokumentoitu, määrittelee auditointien suorittamisen ja suunnittelun. Tietoturvapolitiikasta vastaavan johdon tulee katselmoida tietoturvallisuuden hallintajärjestelmä ennalta suunnitellun ohjelman mukaan tietyin väliajoin. Suositeltavaa olisi tehdä katselmointi kerran vuodessa. Katselmoinnin avulla varmistetaan hallintajärjestelmän jatkuvuus, soveltuvuus, asianmukaisuus ja vaikuttavuus. Katselmuksen tulokset tulee dokumentoida selkeästi. Katselmuksen tulosten perusteella tehdään tarpeelliset parannukset ja muutokset tietoturvallisuuden hallintajärjestelmään. (SFS 27001 2006, 26.)

2.5.3 Fyysinen turvallisuus

Fyysinen turvallisuus koostuu tilojen ja niihin sijoitettujen laitteiden suojaaminen mm. tulipaloilta ja muilta fyysisiltä uhilta. Muita uhkia voivat olla ilkivalta

ja murrot. Toisaalta uhat voivat olla erilaisia ympäristöuhkia kuten vesivahingot tai palovahingot. Sähkökatkoksista tai lämmitysjärjestelmistä aiheutuvia toimintaongelmia vastaan on myös suojauduttava. (Laaksonen ym. 2006, 125–127; Hakala ym. 2006, 11; SFS 27001 2006, 38.)

Fyysisellä turvallisuudella pyritään takaamaan organisaatiolle häiriötön ja turvallinen toimintaympäristö. Toimitilojen suojaamisella luodaan perusta kaikille eri suojaustoiminnoille, joita tietoturvan ylläpitämiseen käytetään. (Laaksonen ym. 2006, 125–127; Hakala ym. 2006, 11; SFS 27001 2006, 38.)

Fyysinen turvallisuus pitää sisällään kaikki ne asiat, joilla pyritään estämään tietojen tuhoutuminen, vahingoittuminen tai tietojen joutuminen vääriin käsiin. Kannettavat tietokoneet ovat muodostaneet vakavan tietoturvaongelman tai pikemminkin niihin kohdistuvat varkaudet. Toisaalta varkaudet kohdistuvat yhä useammin tietokoneen sisältämiin komponentteihin, kuten kovalevyihin, muistipiireihin ja muistikortteihin. Varkaudet tapahtuvat usein keskellä päivää, jolloin eri hälytysjärjestelmät eivät ole päälle kytkettyinä. (Laaksonen ym. 2006, 125–127; Hakala ym. 2006, 11; SFS 27001 2006, 38.)

Tietoturvan kannalta keskeistä on laitetiloihin ja muihin tietojenkäsittelytiloihin pääsyn valvonta. Valvonta pitää ulottaa myös koskemaan työaikaa. Varsinkin laitetilan osalta kannattaisi laatia luettelo niistä henkilöistä, joilla on avaimet laitetilaan. Tällöin tulee ottaa huomioon niin sähköiset järjestelmät kuin fyysiset avaimet, joita voi olla mm. eri pelastusviranomaisilla ja huoltohenkilöstöllä. (Laaksonen ym. 2006, 125–127; Hakala ym. 2006, 11; SFS 27001 2006, 38.)

Taulukossa 2 sivulla 21 kuvataan toimenpiteet joilla estetään omaisuuden häviäminen, vahingoittuminen, varastaminen tai vaarantuminen sekä organisaation toiminnan keskeytyminen (SFS 27001 2006, 39–40).

Taulukko 2. Laitteistoturvallisuus.

Kohde tai toimenpide	Turvamekanismi
Laitteiden sijoitus ja suojaus	Laitteistot tulee sijoittaa tai suojata niin, että ympäristövaarojen ja luvattoman tunkeutumisen riskejä vähennetään.
Peruspalvelut	Laitteistot tulee suojata sähkökatkoilta ja muilta peruspalveluiden katkosten aiheuttamilta häiriöiltä.
Kaapeloinnin turvallisuus	Sähkökaapelointi sekä tietoja siirtävä tai tietotekniikkapalveluita tukeva tietoliikennekaapelointi tulee suojata salakuuntelulta ja vaurioilta.
Laitteiden huolto	Laitteistoja tulee huoltaa asianmukaisesti käytettävyyden ja eheyden ylläpitämiseksi.
Toimitilojen ulkopuolelle vietyjen laitteiden turvallisuus	Turvallisuuden tulee koskea toimitilojen ulkopuolella olevia laitteita ottaen huomioon erilaiset organisaation tilojen ulkopuolella työskentelyyn liittyvät riskit.
Laitteistojen turvallinen käytöstä poistaminen	Kaikki tallennettua tietoa sisältävät laitteet tulee tarkistaa, jotta voidaan varmistua siitä, että arkaluonteinen tieto ja tekijänoikeuden suojaamat ohjelmat on poistettu tai tuhottu turvallisesti ennen käytöstä poistamista.
Suojattavien koneiden siirtäminen pois työpaikalta	Laitteita, tietoaineistoa tai ohjelmia ei saa siirtää pois työpaikalta ilman ennalta saatua valtuutusta.

2.5.4 Henkilöturvallisuus

Standardin SFS 27001 (2006) mukaan on työnantajan ennen työsuhteen alkua varmistuttava siitä, että työntekijät ja ulkopuoliset käyttäjät ymmärtävät velvollisuutensa ja että he ovat sopivia heille tarkoitettuihin työtehtäviin. Samalla vähennetään varkauksien, petosten ja väärinkäytöksien vaaraa. Työntekijöiden taustat tulee tarkistaa noudattaen asiaan liittyviä lakeja ja säädöksiä sekä eettisiä normeja. Tarkistukset tulee suhteuttaa kulloisiinkin liiketoimintavaatimuksiin. Työsuhteen aikana tulee varmistua siitä, että toimijat ovat tietoisia tietoturvallisuuteen kohdistuvista uhista ja niiden merkityksestä. Toi-

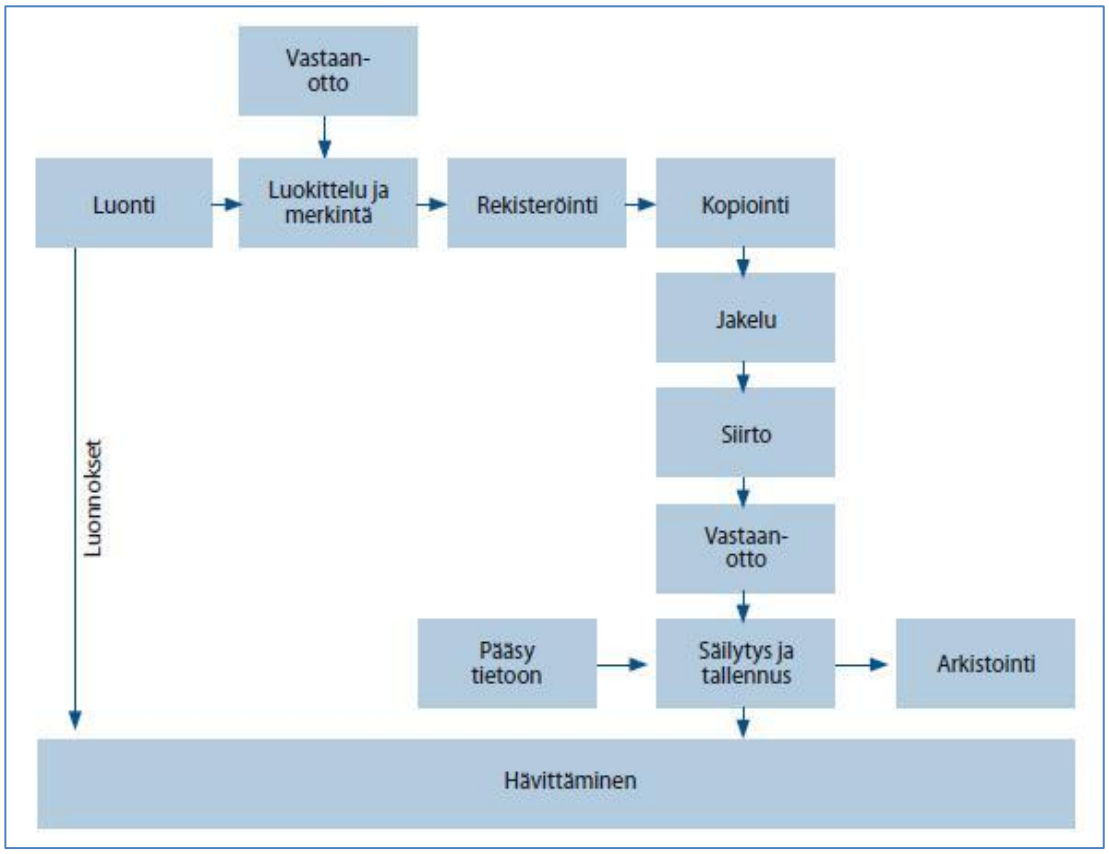
mijoiden tulee olla tietoisia omista velvollisuuksistaan ja vahingonvastuistaan. Lisäksi heillä tulee olla käytössään keinot, joilla he voivat tukea organisaation turvallisuuspolitiikkaa tehdessään normaalia työtään. Työsuhteen päättyessä tulee varmistua siitä, että kaikki toiminnot on tehty järjestelmällisesti. (SFS 27001 2006, 36.)

Hakala ym. (2006) määrittelevät henkilöturvallisuuteen kuuluvaksi ne toimenpiteet, joilla varmistetaan tietojärjestelmän käyttäjien kyky toimia ja toimet, joilla rajataan heidän käyttöoikeuksia käyttää organisaation tietoja ja tietojärjestelmiä. Näitä varmistustoimenpiteitä ovat mm. varahenkilöjärjestelyt, tietoturvaan ja tietojärjestelmiin liittyvät koulutukset, vastuiden ja oikeuksien määrittely ja tietyissä tapauksissa mahdollisten työntekijöiden taustatietojen selvittäminen. Henkilöturvallisuudesta vastaa organisaation henkilöstöhallinto yhteistyössä tietohallinnon ja muiden turvallisuuselinten kanssa. (Hakala ym. 2006, 11.)

Laaksosen ym. (2006) mukaan henkilöturvallisuudella tarkoitetaan henkilöstöön kohdistuvia tietoturvauhkien hallintaa ja henkilöstön toimista aiheutuvien tietoturvauhkien hallintaa. Vaaralliset työyhdistelmät aiheuttavat tietoturvaongelman. Niiden ehkäisemiseksi toimenkuvien tulee olla selkeitä ja vastuiden rajattuja. Henkilöstöhallinnon prosessit lähtien palkkauksesta, työtehtävien muutoksista ja työsuhteen päättymiseen ovat osa henkilöturvallisuuteen liittyviä tilanteita ja riskitekijöitä. (Laaksosen ym. 2006, 138–144.)

2.5.5 Tietoaineistoturvallisuus

Kuviossa 5 kuvataan ne toimenpiteet, joilla turvataan tietojen säilyminen, varmistaminen ja palauttaminen. Myös tuhoamiseen liittyvät toimet ovat osa tietoaineistoturvallisuutta. Tietoaineistoturvallisuuden piiriin kuuluvat myös manuaalisen tietojenkäsittelyn tulosteet siinä missä automaattisen tietojenkäsittelyn avulla tuotetut tulosteet. Tietohallinto ja organisaation arkistotoimi vastaavat tietoaineistoturvallisuudesta yhdessä. (Hakala ym. 2006, 11; Valtionvarainministeriö 2011.)



Kuvio 5. Tietopääoman hallinta (mukaillen Valtionvarainministeriö 2011)

Tiedon luokitus on keskeinen tekijä puhuttaessa tietoaineistoturvallisuudesta. Tieto tulee luokitella mm. sen arvon ja lakisääteisten vaatimusten perusteella. Muita luokitteluperusteita ovat tiedon arkaluonteisuus ja kriittisyys. Tiedon merkitseminen ja käsittely tulee perustua asianmukaiseen ohjeistoon, joka tulee laatia ja ottaa käyttöön organisaation luokitteluperiaatteiden mukaisesti. (SFS 27001 2006, 34.)

2.5.6 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus sisältää ohjelmistoihin liittyviä asioita kuten ohjelmistojen testaus, jolla pyritään varmistamaan sovellusten soveltuvuus haluttuun käyttötarkoitukseen, niiden luotettavuus ja virheettömyys sekä keskinäinen yhteensopivuus. Ohjelmistoversioiden ja lisenssien hallinnointi on olennainen osa ohjelmistoturvallisuutta. (Hakala ym. 2006, 11–12.)

ISO 27001 -standardi vaatii ylläpitämään IT-omaisuusrekisteriä. Parhaiten tämä onnistuu laatimalla lisenssien ja laitteiden hallinnan prosessi. Uudet laitteet ja ohjelmistolisenssit tulee päivittää ko. rekisteriin siinä vaiheessa, kun ne on toimitettu organisaatioon. (Laaksonen ym. 2006, 152–153.)

Muita standardin ISO 27001 asettamia vaatimuksia ohjelmistoturvallisuudelle ovat organisaation ohjelmistopolitiikan laatiminen. Organisaatiossa sallitut ja kielletyt ohjelmistot tulee listata. Haittaohjelmista suojautuminen määritellään myös ko. standardissa. Henkilöstön kouluttaminen nostetaan standardissa esille. Henkilöstöä on ohjeistettava kirjallisesti ja suullisesti ohjelmistojen turvallisesta käytöstä, päivityksien asentamisesta sekä esimerkiksi arkaluonteisten tietojen salaamisesta. Standardi edellyttää tekemään myös järjestelmien kuvaukset. Esimerkiksi palvelinympäristön tietoturvan lisäämiseksi tehdyt asetusmuutokset on dokumentoitava ja ohjeistettava ylläpitäjille. Varmuuskopiointikäytännöt ja niiden ohjeistukset on dokumentoitava ja tarpeen mukaan julkaistava myös henkilöstölle. Standardi edellyttää, että on dokumentoitava mahdolliset ohjelmistoihin liittyvät tukisopimukset ja niihin liittyvät avunpyyntöperiaatteet. (SFS 27001 2006, 29–31.)

2.5.7 Laitteistoturvallisuus

Laitteistoturvallisuuden tavoitteena on standardin SFS 27001 (2006, 38) estää omaisuudelle tapahtuvat vahingot, joita voivat olla omaisuuden häviäminen, vahingoittuminen tai varastaminen. Laiteturvallisuudesta huolehtimalla varmistetaan organisaation toiminnan jatkuminen. Laiteturvallisuuteen voidaan vaikuttaa laitteiden sijoittelulla ja suojauksella, joilla pyritään torjumaan ympäristövaaroja ja luvattomien tunkeutumisen riskejä. Muita keinoja parantaa laiteturvallisuutta ovat niiden suojaaminen sähkökatkoksilta. Sähkökaape-

lointiin ja tietoliikennekaapelointiin tulee suojata mm. salakuuntelulta ja fyysisiltä vaurioilta. Laitteiston huolto tulee toteuttaa säännöllisesti käytettävyyden ja eheyden ylläpitämiseksi. Laitteiden poistaminen käytöstä on myös osa laitteistoturvallisuutta. Poiston yhteydessä tulee varmistua siitä, että kaikki arkaluontoinen ja salassa pidettävä tieto on poistettu poistettavasta laitteesta. Ohjelmia, laitteita tai tietoaineistoja ei saa siirtää pois työpaikalta ilman valtuutusta. (SFS 27001 2006, 38.)

Laitteistoturvallisuudessa tulee ottaa huomioon myös laitteiden matka- ja kotikäytön aiheuttamat riskit. Laitteiden matka- ja kotikäyttö edellyttää, että organisaation ulkopuolella työskentelyn riskit on huomioitu ja niiden edellyttämät turvamekanismit on otettu käyttöön. Laitteiden, ohjelmistojen ja tietojen vieminen pois organisaation tiloista edellyttää erillistä lupaa. (Hakala ym. 2006, 308.)

2.5.8 Tietoliikenneturvallisuus

Tiedonsiirtojärjestelmät kuten lähi- ja laajaverkkoyhteydet kuuluvat tietoliikenneturvallisuuden piiriin. Tietoliikenneturvallisuudessa huolehditaan myös muiden viestintäjärjestelmien toiminnasta. Toiminnosta vastuussa on yleensä organisaation tietohallinto. (Hakala ym. 2006, 12.)

Standardissa SFS 27001 kuvataan verkon turvallisuuden hallinta, jonka tavoitteena on verkossa kulkevan tiedon ja tukena olevan verkon rakenteen suojauksen varmistaminen. Riittävä verkkojen hallinta ja valvonta auttavat suojautumaan uhilta. Lisäksi sen avulla pystytään ylläpitämään verkkoa käyttävien sovellusten ja järjestelmien sekä niissä liikkuvan tiedon turvallisuus. Verkkopalvelujen turvaaminen, niin sisäisten kuin ulkoistenkin, on osa tietoliikenneturvallisuutta. Turvallisuusominaisuuksien ja palvelutason yksilöinti sekä niiden sisällyttäminen verkkopalvelusopimuksiin on tärkeää. (SFS 27001 2006, 42.)

Etäkäyttötekniikat mahdollistavat etäkäyttäjän, internet-/intranet -käyttäjien sekä ekstranet -käyttäjien liittymisen organisaation hallinnoimaan verkkoon. Etäkäyttötekniikoiden avulla varmistetaan tietojen luottamuksellisuus, käytettävyys ja eheys. Näiden tekniikoiden hallinta ja toimivuus on keskeinen osa tietoliikenneturvallisuutta. (Krutz–Vines 2003, 118.)

2.6 Etätyö ja tietokoneen matkakäyttö

Etätyöllä tarkoitetaan työnteon muotoa, jossa työ tehdään joko osin tai kokonaan kotona tai muussa työntekijän valitsemassa paikassa ja se nähdään yhteä keinona nykyaikaistaa työn organisointia ja sovittaa yhteen työ- ja vapaa-aika. Etätyötä kutsutaan usein e-työksi, koska siinä hyödynnetään usein tieto- ja viestintätekniikkaa. Etätyöstä voidaan käyttää myös nimitystä hajautettu työ tai liikkuva työ. (Työ- ja elinkeinoministeriö 2010, Kuntatyönantaja 2010.)

Etätyön avulla halutaan parantaa työn tuottavuutta ja työelämän laatua. Työssä jaksaminen, työn ja perhe-elämän yhteensovittaminen, työ- ja asuinpaikan joustava sijoittuminen ovat myös merkittäviä etuja puhuttaessa etätyöstä. Etätyön tekeminen vähentää matkakustannuksia ja siihen käytettävää aikaa. (Työ- ja elinkeinoministeriö 2010, Kuntatyönantaja 2010.)

Suomessa tehdään e-työtä vaihtelevasti sekä sovittuina että epävirallisina järjestelyinä. Suomen hallitus on hyväksynyt vuonna 2006 periaatepäätöksen etätyön edistämiseksi. Työmarkkinajärjestöt ja valmistelevat ministeriöt ovat olleet mukana periaatepäätöksen valmistelussa. Suomessa suuntaus näyttää olevan se, että työympäristössä siirrytään kohti vaihtelevia ja monipuolisempia työaikoja ja -paikkoja. (Työ- ja elinkeinoministeriö 2010, Kuntatyönantaja 2010.)

Tietoliikenneturvallisuuden avulla mahdollistetaan etätyön tekeminen. Erilaisten turvallisten etäkäyttötekniikoiden avulla etätyöntekijät voivat muodostaa yhteyden työnantajan tietoverkkoon. (Krutz–Vines 2003, 118.)

Suomen kuntaliiton tekemän selvityksen mukaan teknisesti ja juridisesti etätyöhön on mahdollisuus noin 41 prosentilla selvitykseen osallistuneista kuntien työntekijöistä ja 40 prosenttia kentällä liikkuvaa työtä tekevistä oli mahdollisuus käyttää tarvitsemiaan tietojärjestelmiä etäyhteydellä. (Kettunen 2010, 6.)

Työnantajan tulee määritellä ne toimintaperiaatteet ja turvamekanismit joiden avulla suojaudutaan riskeiltä, joita etätyö ja tietokoneen matkakäyttö saattavat aiheuttaa (SFS 27001 2006, 50).

Etätyöhön ja tietokoneen matkakäyttöön liittyviä riskejä ovat laitteen unohtuminen eri paikkoihin, julkisella paikalla olanylikatselu tai jopa näytön valokuvaaminen, langattomien verkkojen suojaus voi olla puutteellinen ja laitteen varastaminen. Riskejä voidaan pienentää ohjeistamalla käyttäjää siitä, missä laitetta voi käyttää ja millaista tietoa laitteessa saa säilyttää. Kannattaa pohtia myös laitteen tietojen varmistamismahdollisuuksia. (Laaksonen, ym. 2006, 168–169.)

2.7. Sähköinen asiointi julkishallinnossa

Laki sähköisestä asioinnista viranomaistoiminnassa on tullut voimaan vuonna 2003. Lain tavoitteena on, että viranomaistoiminnassa voitaisiin siirtyä laajalti käyttämään sähköistä asiointia. Lakia sähköisestä asioinnista hallinnossa sovelletaan hallintoasian, tuomioistuinasian ja ulosottoasian sähköiseen vireillepanoon, käsittelyyn ja päätöksen tiedoksiantoon, jollei toisin säädetä. Sähköistä asiointia viranomaistoiminnassa koskevan lain 2 luvun 5 §:n mukainen kuntien velvollisuus tarjota mahdollisuus sähköiseen asian vireille saattamiseen koskee vain niitä kuntia, joilla on tarvittavat tekniset, taloudelliset ja muut valmiudet vireillepanon toteuttamiseen. Vastaanottokuittaus ja saavutettavuusvelvoite koskevat kaikkia kuntia, jotka käyttävät edellä mainittua sähköistä asiointia. (Laki sähköisestä asioinnista viranomaistoiminnassa 2003; Suomen kuntaliitto 2003.)

Sähköinen asiointi on lisääntynyt Suomen kunnissa. Verkon kautta voi hoitaa yhä useampia asioita. Kirjastot ovat olleet etunenässä kehittämässä sähköisiä palveluitaan. Lisäksi monet lomakkeet ja mm. tilojen varaukset ovat tarjolla verkossa. Myös monimutkaisempien asioiden, kuten päivähoitopaikan varaaminen onnistuu jo useilla paikkakunnilla. Euroopan mittakaavassa Suomi on sähköisen asioinnin kärkimaita. Suomessa voi esimerkiksi täyttää veroilmoituksen verkossa käyttäen pankkien antamia sähköisen palvelun pankkitunnisteita. Sähköisen asioinnin uskotaan lisäävän kuntalaisten tyytyväisyyttä kunnallisiin palveluihin. Samalla sen uskotaan tuovan säästöjä kuntatalou-

teen ja sen avulla varmistetaan palveluiden saatavuus. (HighTech Forum Oulu 2007.)

Suomen kuntaliitto (2010) on ohjeistanut viranhaltijoita sähköiseen asiointiin liittyen. Ohjeissa otetaan kantaa mm. seuraaviin asioihin:

- Miten saapuvien sähköisten asiakirjojen kirjaaminen järjestetään?
- Miten tulee menetellä kunnan viranhaltijoiden sähköpostiin tulleiden sähköisten asiakirjojen kanssa?
- Kenellä on vastuu viestin perille menosta?
- Millainen vastaanottoilmoituksen tulee olla ja mikä on vastaanottoilmoituksen merkitys?
- Voiko luottamushenkilö ilmoittaa erostaan sähköpostitse?
- Onko sähköpostitse tullut työhakemus huomioitava hakuprosessissa?

3 TUTKIMUSMENETELMÄT JA AINEISTO

3.1 Tutkimusmenetelmät

Oikean tutkimusmetodin valinta on keskeisin asia empiirisessä tutkimuksessa. Käytettävän metodin soveltuvuutta tutkimusongelmien ratkaisemiseen on tällöin mietittävä tarkasti. Tutkimusmetodin on käytännöllinen silloin, kun se on yhtenevä teorian, hypoteesin ja metodologian kanssa. (Metsämuuronen 2000, 9–10.)

Tutkimusmetodin valintaan vaikuttaa myös se, millaista tietoa haetaan ja keneltä ja mistä sitä haetaan. Valitsin tutkimuksen haastattelumenetelmäksi teemahaastattelun, koska se mahdollistaa tutkijalle lisäkysymysten tekemisen haastattelun aikana. Haastattelut toteutettiin haastateltavien omissa työhuoneissa, kuitenkin siten, että haastattelutilanteen keskeytymisen vaaraa ei ollut. (Saaranen-Kauppinen & Puusniekka 2006.)

Tässä tutkimuksessa tutkittavien kohteiden omat kertomukset ja näkemykset sekä aineisto olivat keskeisellä sijalla. Haastateltavat saivat vapaasti, teemojen puitteissa, kertoa omia näkemyksiään ja kokemuksiaan tutkittavasta aiheesta.

Teemahaastattelun avulla on tarkoitus selvittää, mitä haasteltavat ajattelevat käsiteltävistä teemoista. Haastattelussa, joka on eräänlainen keskustelutilanne. Haastattelutilanteessa tutkija toimii aloitteentekijänä ja ohjailee haastattelua haastatteluteemojen mukaisesti. Puhumisjärjestys on vapaamuotoinen ja kaikkien haastateltavien kanssa ei käydä kaikkia teemoja yhtä laajasti läpi. (Eskola-Suoranta 1996.)

Haastateltaville on hyvä kertoa etukäteen haastattelun tarkoitus ja haastattelumenetelmä, näin voidaan poistaa ennakkoasenteita haastattelua kohtaan. Tutkimuksessani haastateltavat tiesivät ennakkoon, että tulen nauhoittamaan haastattelut, jotka sitten myöhemmin tullaan purkamaan eli litteroimaan. Heillä oli tieto myös haastattelun teemoista yleisellä tasolla. Haastattelun kuluessa kerroin haastateltaville tietoturvan eri osa-alueet sekä tietoturvaan liittyvän ohjeiston otsikkotasolla ennen syvällisempää alueiden läpikäyntiä.

Teemahaastattelu etenee vaiheittain siten, että ensimmäisessä vaiheessa tutustutaan huolella tutkittavaan aihepiiriin ja valitaan teemat. Toisessa vaiheessa laaditaan teemahaastattelun runko. Kolmanteen vaiheeseen kuuluu haastattelun toteuttaminen. Neljännessä vaiheessa kirjoitetaan nauhoitettu aineisto tekstiksi eli suoritetaan litterointi. Tämän jälkeen suoritetaan aineiston luokittelua ja analysointia. Viimeisessä vaiheessa julkaistaan tutkimustulokset eli tehdään raportti. Haastateltavat on valittava huolella siten, että heillä arvellaan olevan parhaiten tietoa tutkittavasta asiasta. (Saaranen-Kauppinen & Puusniekka 2006.)

Tässä tutkimuksessa haastateltaviksi valittiin kunnan eri osastojen osastopäälliköt, jotka käytännössä vastaavat tietoturvapolitiikan käytännön toteutuksesta tutkimuskohteessa. Teemojen suunnittelu vaati perehtymistä tietoturvallisuuden standardeihin, alan kirjallisuuteen ja tutkimuskohteen tietoturvapolitiikkaan.

3.2 Aineisto

Aineiston analysointivaiheessa selvitetään, millaisia vastauksia tutkimusongelmaan on saatu. Aineistosta pyritään luomaan mielekästä, selkeää kokonaisuutta, joka kasvattaa aineiston informaatioarvoa. Kvalitatiivisen aineiston analyysissä yhdistyvät analyysi ja synteesi, jolloin tätä vaihetta voidaan kutsua abstrahoinniksi, jolla tarkoitetaan tutkimusaineiston järjestämistä. Aineisto järjestetään siihen muotoon, että sen perusteella tehdyt johtopäätökset voidaan irrottaa yksittäisistä tekijöistä ja siirtää ne käsitteelliselle ja teoreettiselle tasolle. (Grönfors 1982, 145.)

Yhtenä aineiston analyysin tarkoituksena on aineiston tiivistäminen ja muokkaaminen paremmin käsiteltävään muotoon (Kylmä–Juvakka 2007, 66).

Tutkimuksessani lähdin analysoimaan aineistoa siten, että ensin kuuntelin kertaalleen läpi nauhoittamani haastattelut. Kuuntelun jälkeen litteroin haastattelut. Luokittelin haastateltavien vastaukset teemoittain. Tällä luokittelulla luotiin pohja haastatteluaineiston tulkinnalle.

Analyysin tekeminen voidaan luokitella kolmeen eri malliin, aineistolähtöiseen, teoriasidonnaiseen tai teorialähtöiseen analysointimalliin (Metsämuuronen 2005, 213–214). Tutkimuksessani aineiston analysointi oli merkittävässä roolissa.

Suoritin luokittelun käytännössä tekstinkäsittelyohjelmaa hyödyntäen. Luokiteltu tutkimusaineisto kertoi, mitä mieltä haastateltavat olivat kysytyistä asioista. Luokittelun jälkeen esitin tutkimuksen tulokset, jotka on kuvattu tämän tutkimuksen luvussa 4. Mainittakoon, että käsittelin hallinnollisen tietoturvallisuuden luvussa (4.4), koska se on keskeinen osa tietoturvallisuuden johtamistoimintoa ja se muodostaa lähtökohdan organisaation koko tietoturvatoiminnalle (SFS 27001 2006, 14–20).

Analyysin ja tutkimustulosten jälkeen vertasin keskeisimpiä tutkimustuloksia tietoturvastandardiin SFS 27001 (2006) sekä alan auktoriteettien kirjallisiin lähteisii.

Haastattelujen sisällön analysoinnin luotettavuuteen vaikuttavat tutkija itse, aineiston laatu ja sen analyysi sekä tutkimustulosten esittely. Aineiston ja tutkimustulosten välinen yhteys on analyysissä tärkeää. Keskeinen haaste on, miten pystyy pelkistämään ja tiivistämään aineistoa niin, että se kuvaa mahdollisimman luotettavasti tutkittavaa ilmiötä. (Latvala–Vanhanen–Nuutinen 2003, 36.)

4 TIETOTURVAKÄYTÄNNÖT TUTKIMUSKOHTEESSA

4.1 Tieturvapolitiikkaan liittyvät ohjeet tutkimuskohteessa

Tutkimuskohteessa kunta on toteuttanut yhdessä konsulttiyhtiön kanssa tietoturvan hallinnan- ja kehittämisprosessin vuosien 2005–2007 aikana. Tietoturvan hallinta on osa kunnan laatujärjestelmää ja hankkeen tavoitteena on ollut nostaa henkilöstön tietoturvan hallinnan tasoa ja tehdä kattava tietoturvakartoitus. Hankkeen tavoitteena on ollut toteuttaa koko kunnan organisaatiota koskeva tietoturvan hallinnan järjestelmä. (Kohdekunta 2007b.)

Kehittämishankkeessa toteutettiin tietoturvakartoitus, joka dokumentoitiin yksityiskohtaisesti. Kartoitus perustuu ISO 27001 -standardin asettamiin vaatimuksiin. Tämän lisäksi laadittiin ohjeistukset tietojärjestelmien hallinnointiin, tietojen ja asiakirjojen luokitteluun, tietoturvaan, tietosuojaan, tietoturvapoikkeaman käsittelyyn ja etätyöhön. Lisäksi henkilökunnalle laadittiin tietoturvallisuuden huoneentaulu. (Kohdekunta 2007b.)

Tutkimuskohteessa tietoturvapolitiikasta vastaa kunnanhallitus yhdessä kunnanjohtajan kanssa. Kunnanhallitus yhdessä kunnan johdon kanssa määrittävät tietoturvapolitiikan avulla tietoturvallisuuden tavoitteet, vastuut ja toteutuskeinot. Kunnanhallitus on vahvistanut nämä periaatteet 29.5.2007. (Kohdekunta 2007a.)

Tietoturvapolitiikka -asiakirjassa kuvataan tutkimuskohteen tietoturvapolitiikka, jonka avulla määritellään tietoturvallisuuden tavoitteet, vastuut ja toteutuskeinot. Kunnan tietototurvasta vastaavat kunnanhallitus ja kunnanjohtaja. Tietoturvapäällikkönä toimii kunnankamreeri, joka vastaa tietoturva-asioiden tiedottamisesta. Osastojen tietoturvatoimenpiteiden organisoinnista ja toimeenpanosta vastaavat osastopäälliköt. Kunnan tietosuojavastaavana toimii keskusarkistonhoitaja. Atk-päällikkö vastaa tietoturvan toteuttamisesta ja järjestelmien ylläpidosta sekä antaa tietoturvallisuuteen liittyviä ehdotuksia. (Kohdekunta 2007d.)

4.2 Käsitteen tietoturva ymmärtäminen

Osastopäälliköt kuvasivat vastauksissaan tietoturvaan liittyvää kolmea suurta periaatetta: luottamuksellisuutta, eheyttä ja käytettävyyttä seuraavasti.

> *Tietoturvasta tulee mieleen tietojen, ensinnäkin tietojen kirjain - paperilla olevan tiedon säilyttäminen jossakin. Yhtälailla myös sähköpostin ja muun tiedon säilyttäminen, tallentaminen. Myöskin siihen liittyy minun mielestä salassapitoasiat*. (V4)

> *Mä ymmärrän sen sen niinko säilyttämisen kannalta, että asiat säilytetään sillätavalla, että ne pysyy säilytyksessä, pysyy turvassa. Sit siihen liitty tämmönen salassapito, et on tiettyjä asioita, jotka pitää säilyttää niin, ettei niihin kukaan pääse. Sit mulle kyllä tietoturvasta tulee myös se mieleen, että tämmöset haasteet, että mikä on sitten semmosta niinku salasta ja tuota mikä on semmosta tietoa sitten, että joka on niinko, joka pitäis olla kaikille niinko saatavilla.* (V3)

Tietoturvan eri osa-alueet tulivat tässä vaiheessa esiin kahden haastateltavan vastauksissa.

> *Tietoturva on niinku …sana tietoturva tarkoittaa tiedon turvaamista mut tota lähinnähän se nyt ymmärretään niiku tässä kunnan organisaatiossa kunnan tietojen salaamisjärjestelmää ja se että ne joudu vieraisiin käsiin…..mutta siihen liittyy tämmönen muukin tilojen turvallisuus …. tietysti tähän tiedon turvaamiseen sitten tietysti … Oisko tämä henkilöturvallisuus sitten yksi tekijä myös? Ja ja mitähän lie muuta, jotakin muutakin varmaan …. Laaja käsite sinänsä*. (V1)

> *No tuota sen voi esittää suppeasti tai laajasti. Elikkä minä ajattelin, että se tietoturva ei oo ainoastaan tämä sähköinen vaan se on ihan kaikki paperilla ja suullisesti ja kaikki tämmönen. Ja se voi olla niinku asiakirjoihin liittyvää ja tämmöstä näin, että niin. Yleensä semmonen että tuota ei menis semmosta tietoa mikä ei kuulu sivullisille eikä sitä tietoa väärin käytettäis elikkä tietoa ja ym. mitä siellä onkaan. Niin minä ajattelin et se on hirviän laaja. Et ei ainoastaan liity näihin masiinoihin*. (V2)

Haastateltaville muodostunut kuva käsitteestä tietoturva vaihteli. Käsite ei kuitenkaan ollut täysin vieras, vaan haasteltavat tiesivät siitä joitakin ominaisuuksia ja osa-alueita. Pitää kuitenkin muistaa, että tietoturvan eri osa-alueiden muodostaman kokonaisuuden hallinta on laadukkaan tietoturvajohtamisen edellytyksenä.

4.3 Haastateltavien tietoturvan eri osa-alueiden tuntemus

4.3.2 Fyysinen turvallisuus

Tilojen ja niihin sijoitettujen laitteiden suojaaminen mm. tulipaloilta ja muilta fyysisiltä uhilta sekä siihen, että pyritään takaamaan organisaatiolle häiriötön ja turvallinen toimintaympäristö kiinnitti huomiota yksi haasteltavista.

Tietoturvan kannalta keskeistä on laitetiloihin ja muihin tietojenkäsittelytiloihin pääsyn valvonta. Tähän viittaavat asiat tulivat esille kolmen haastateltavan vastauksissa.

> *Kulunvalvontahan on tietysti käytössä että siinä on niinku sisääntulot ja lähdöt talosta kirjautuu ylös ja muutkin pitempiaikaiset poissaolot mut tota mitähän muuta siihen voisi sisältyä?* (V1)

> *No silleen suojataan tietysti että .. tarkoitat lukituksia … niin niin siihen on aika tarkat ohjeetkin että tilat on pidettävä lukittuna jos henkilö ei ole paikalla toimistossa että siinä mielessä ohjeet on ainakin yksiselitteiset ja kyllä näyttävät toimivankin aika hyvin että ovi on lukossa, jos henkilö ei ole paikalla.* (V1)

> *No meillä on nyt aika tavallakin kiinnitetty siihen huomiota. Elikkä meillä on tämä kulkeminen täällä huomattavasti vaikeutunut tai tullut turvallisemmaksi tietoturvan kannalta. Elikkä huoneitten ovet pittää olla lukittuna, ko henkilö lähtee pois huoneesta. Ulko-ovet on tietyllä tavalla lukittuna ihan ja sitten on tämä portaatkin suljettu, että me on aika tavalla kiinnitetty tähän huomiota*. (V2)

4.3.3 Henkilöturvallisuus

Työntekijöiden taustat tulee tarkistaa noudattaen asiaan liittyviä lakeja ja säädöksiä sekä eettisiä normeja. Haastateltavien vastauksissa tämä asia nousi esille.

> *Rekrytointi on aika harvinaista .. mutta ko on.. hmmm.. siis hakemuksen yhteydessä pyydetään tietysti tiettyjä henkilötietoja ja opiskeluun liittyviä matariaaleja toimitettavan mutta muuta muuta henkilön rikosrekisteriä tämän typpisiä asioita ei oo kyllä toistaiseksi ainakaan tarkastettu.* (V1)

> *No silloin ku oudompi tai outo ihminen hakee, meille tuntematon ihminen, niin – pääsääntöisesti yhteydenoton hoidan minä. Mutta myös xx. Elikkä tarkistetaan edellisiltä työnantajilta. Se vähän riippuu tapauksesta. Jos ei oo mitään kokemusta niin sitten mahdollisesti otan kahdelta, mutta joskus jopa yksi riittää. Se riippuu vähän siitä työnantajasta, missä hän on ollut.* (V4)

Yksi haastateltavista toi esiin rikosrekisteriotteen vaatimuksen tapauksissa, joissa rekrytoitava työskentelee alaikäisten parissa.

> *Ei muuta ko että. Ei tehä siis tässä tarkoituksessa ei tehä muuten ku, et meillä on se rikosrekisteri ote pyydetään näyttämään, kun palkataan lasten kanssa työskentelemään.* (V3)

Työsuhteen aikana tulee varmistua siitä, että toimijat ovat tietoisia tietoturvallisuuteen kohdistuvista uhista ja niiden merkityksestä. Toimijoiden tulee olla tietoisia omista velvollisuuksistaan ja vahingonvastuistaan. Lisäksi heillä tulee olla käytössään keinot, joilla he voivat tukea organisaation turvallisuuspolitiikkaa tehdessään normaalia työtään. Näihin standardin edellyttämiin toimiin viittasi yksi haastateltava neljästä.

> *Joo. Elikkä tuota. Niin no joo. Kyllä me niinkö annetaan nämä tietoturvaohjeet niille, mitkä meillä on tehty semmonen pieni huoneentaulu ja sitten on semmonen tietoturvapolitiikka. Niin ne annetaan. Sitten niillä pittää tietenkin ne käyttäjälaput täyttää ja sitoutua noudattamaan niitä.* (V2)

4.3.4 Ohjelmistoturvallisuus

Ohjelmistoturvallisuuteen liittyvät asiat olivat haastateltavilla kohtalaisen hyvin hallussa.

Ohjelmistoturvallisuus sisältää ohjelmistoihin liittyviä asioita kuten ohjelmistojen testaus, jolla pyritään varmistamaan sovellusten soveltuvuus haluttuun käyttötarkoitukseen, niiden luotettavuus ja virheettömyys sekä niiden keskinäinen yhteensopivuus. Ohjelmistoversioiden ja lisenssien hallinnointi on olennainen osa ohjelmistoturvallisuutta.

Tutkimuskohteessa ohjelmistoturvallisuutta käsitellään Tietojärjestelmien hallinnointi -asiakirjassa, jonka kunnanjohtaja on hyväksynyt hallintosäännön pohjalta 1.10.2007.

> *No.. Siitä on aika tarkat ohjeet ja se että näihin koneihin on niikö että käyttäjät … varsinaiset käyttäjät eivät pääse ees asentamaan ohjelmia ja netistä kopioimaan ohjelmia … että siinä mielessä asia on aika hyvällä mallilla .. mutta se että kaikki ohjelmis-*

> *tot asennetaan atk-henkilöstön toimesta …. hyvinkin tarkat rajaukset on.* (V1)

> *Joo. Meillähän nämä periaatteessa kaikki ohjelmat ovat näitä valmisohjelmia. Että täällähän ei mitään tehdä ite. Että mehän ostetaan dynstit, rondot.* (V2)

4.3.5 Laitteistoturvallisuus

Laitteistoturvallisuuden tavoitteena on estää omaisuudelle tapahtuvat vahingot, joita voivat olla omaisuuden häviäminen, vahingoittuminen tai varastaminen. Laiteturvallisuudesta huolehtimalla varmistetaan organisaation toiminnan jatkuminen. Laiteturvallisuuteen voidaan vaikuttaa laitteiden sijoittelulla ja suojauksella, joilla pyritään torjumaan ympäristövaaroja ja luvattomien tunkeutumisen riskejä. Muita keinoja parantaa laiteturvallisuutta ovat niiden suojaaminen sähkökatkoksilta.

Laitteistoturvallisuus ja fyysinen turvallisuus liittyvät kiinteästi yhteen. Haastateltavien kokemukset fyysisen turvallisuuden huomioon ottamisesta on kuvattu luvussa 4.3.2 Fyysinen turvallisuus. Tämän lisäksi yksi haastateltavista viittasi sähkökatkosten aiheuttamiin ongelmiin. Sähkökatkoksiin ei ainakaan työasematasolla ole varauduttu.

> *Nooo eihän siis suoraan nää meijän laitteet niin kyllä nää sammuu ku virta lakkaa tulemasta mutta tietysti meillä on tää intranetin puolella nää kuitenkin palavelimet on suojattu ja että se tieto, mikä yleensä tallennetaan sinne verkon palvelimille ja sitä kautta ne on niinku kaikki nauhotukset tapahtuvat. En tiiä tekeekö kaikki niin mutta semmonen itse henkilökohtaisesti teen niin että verkkolevyä käytän. Ja sitten sähkökatkokset.. siellähän on varauduttu kyllä että siellä lyhyet sähkökatkokset koneet ehditään ajaa alas että tieto säily ja että nauhotukset toimii tietääkseni ihan ..ihan asianmukaisesti*. (V1)

4.3.7 Tietoaineistoturvallisuus

Tietoaineistoturvallisuus kattaa ne toimenpiteet, joilla turvataan tietojen säilyminen, varmistaminen ja palauttaminen. Tietohallinto ja organisaation arkistotoimi vastaavat tietoaineistoturvallisuudesta yhdessä.

Haastateltavien vastauksissa nousi esille tietokoneille ja palvelimille tallennetun tiedon varmistaminen. Nämä varmistustoimet hoitaa kunnan atk-osasto.

> *Ja meillä on niinkotuota ne varmistukset, niin tuota hoietaan tuonne verkon levylle.* V2

> *No jos kävis niin ikävästi, että tietokoneelta joutuis kaikki tieto hukkaan, niin onhan meillä olennaiset asiat, jos nyt xx asoista puhutaan, niin onhan ne paperilla.* (V4)

Tiedon luokitus on keskeinen tekijä puhuttaessa tietoaineistoturvallisuudesta. Tieto tulee luokitella mm. sen arvon ja lakisääteisten vaatimusten perusteella tai sen arkaluonteisuus ja kriittisyys perusteella. Organisaatio laatii luokitteluperiaatteet, joiden mukaan tiedon käsittely ja merkitseminen tapahtuu.

Haastateltavien vastuksissa em. periaatteet nousivat esille.

> *”Ooonn… tietysti meillähän käsitellään palavereissa salaisia asioita niin nehän ovat salaisia organisaatiossa talon sisällä niin eihän niihin kuka tahansa voi päästä käsiksi ja vielä vähemmän ulkopuoliset …. niin niin salattavia asioita löytyy mutta hyvin vähän verrattuna moneen muuhun hallintokuntiin.*(V1)

> *Joo. Varmaan monellakin lailla on otettu huomioon. Elikkä tuota esimerkiksi no niissä ohjeissa on kaikenlaista. Avoimessa internetverkossa ei saa lähetellä näitä joissa on tietosuoja. No ensinnäki kaikki lähtee siitä laki…julkisuuslaki ja henkilötietolaki, että mitkä on niinku salassa pidettäviä. (*V2)

4.4 Hallinnollinen turvallisuus

4.4.1 Vastuu tietoturvapolitiikasta tutkimuskohteessa

Hallinnollinen tietoturvallisuus on keskeinen osa tietoturvallisuuden johtamistoimintoa ja se muodostaa lähtökohdan organisaation koko tietoturvatoiminnalle. Se muodostuu periaatteista, jonka organisaation johto on hyväksynyt. Kunnallisessa organisaatiossa kyseessä on johtosäännön mukainen päätöksentekojärjestys. Hallinnollisessa tietoturvassa on kysymys myös vastuunjaosta, resurssien varaamisesta sekä riskien arvioinnista. Hallinnollisen tietoturvan avulla luodaan organisaatiolle tietoturvalliset toimintatavat ja toimintamallit.

Tutkimuskohteessa tietoturvapolitiikasta vastaavat kunnanhallitus ja kunnanjohtaja. Käytännön tietoturvapolitiikan toimeenpano on osastopäälliköiden vastuulla.

Haastateltavat tiesivät varsin hyvin sen, kuka vastaa tietoturvapolitiikasta tutkimuskohteessa.

> *Kunnanjohtaja tietysti … kun tietysti organisaation ylimmästä päästähän sitä lähetään… sitten sitä on pilikottu pienempiin osiin ja sitten se on meillä osastopäälliköillä omat roolimme .. johdostahan se lähetään kunnanjohtaja – kunnanhallitus, sitten on atk-osasto ja sitten osastopäälliköt.* (V1)

> *Kunnanhallitus ja kunnanjohtaja.* (V2)

> *Osastopäälliköt niistä omista osastoistaan kyllä. Mut ihan koko kunnan tasolla olen ymmärtänyt, et se olis XX, mutta ilman muuta osastopäälliköt. niinkö minä xx -toimessa. Tai se on nyt jaettu tässä ku nää toimintayksiköt sijaitsee fyysisesti erillään.*(V3)

4.4.2 Tietoturvapolitiikkaan liittyvien ohjeistojen tunteminen

Tutkimuskohteessa on laadittu tietoturvapolitiikkaan liittyen seuraavat ohjeistot; Tietojärjestelmien hallinnointi, Tietoturvaohje, Tietosuojaohjeisto, Tietojen ja asiakirjojen luokittelu, Etätyöohje, Tietoturvapoikkeaman käsittely ja Tietoturvallisuuden huoneentaulu.

Haastateltavista kolme pystyi nimeämään yhden tai useamman tietoturvapolitiikkaan liittyvän ohjeen. Kaikilla haastateltavilla oli kuitenkin tieto siitä, että erilaisia tietoturvaan liittyviä ohjeistoja on laadittu, mutta niiden nimeäminen ei onnistunut haastattelutilanteessa. Tietoturvan huoneentaulu nousi esille kolmen haastateltavan vastauksissa. Yksi haasteltavista mainitsi tietojen ja asiakirjojen luokittelua käsittelevän ohjeen.

> *Joo siinähän on tuota .. tietoturvapolitiikka.. siitä on ohje ja sitte tuota tietoturvan huoneentaulu. Ja nää löytyy meillä intranetistä ja ne on varmaan suht hyvät… tai en tiiä kuinka hyvin tunnettuja mutta sieltä ohjeet ja määräykset siltä osiosta löytyvät intranetin tuolta sisätiestä ja tuota sitten on tarkempi ohjeistus jota ei ole kyllä jaettu henkilöstölle.* (V1)

> *No kyllä minä tunnen nämä ohjeistukset mitä meillä on. Meillä on aikalailla niin tuota. No minä äskettäin sanoinkin, että meillä on henkilöstölle nämä huoneentaulut ja sitten se tietoturvapolitiikka, mikä kunnanhallitus on vahvistanut. Sitten meillä on etätyöohjetta ja ja mitähän siinä kaikkia onkaan* (V2)

Kysyttäessä tarkemmin Tietoturvallisuuden huoneentaulun sisällöstä ja käyttötarkoituksesta haastateltavat vastasivat mm. seuraavasti.

> *No siinä on … tietoturvallisuuden huoneentaulussa on niinko onko se yhellä A4:lla tai kahella lyhyesti kirjoitetut ohjeet niinko tietoverkon käytöstä ja tietotekniikan käytöstä talossa … semmonen niinko huoneen taulun muotoon kirjoitettu tietoturvaohje.* (V1)

> *Niinku sanottu yksinkertasesti, että mitä henkilökunnalta edellytetään, että mitä niien pittää tietää, niinku pähkinänkuoressa tästä tietoturvasta. Että minusta se on aika kattavaki. Mulla se on mapeissa. Sitten meillä löytyy tuosta sisätieltä niin ite kukanenki voi käyä kattomasa niinniintuota tuosta että miten nämä asiat mennee. Sitten aina ku tullee uus henkilö niin niille jaetaan se. Ja sitä käyään tarvittavilta osilta läpikin.* (V2)

> *No on. Se on, se on jossain täällä säännöissä. Oon sen lukenut. Se on siinä säännöissä. Näitä tietoturvaan, mitä sä teet tässä. Päivittäiseen rutiiniin liittyvät ohjeet.* (V4)

4.4.3 Työnantajan järjestämä tietoturvaan liittyvä tiedotus ja koulutus

Tutkimuskohteen tietoturvapolitiikka lähtee siitä, että henkilökunnalle kohdennetulla ohjeistuksella, koulutuksella ja tiedottamisella varmistetaan se, että henkilökunnalla on riittävät valmiudet tietoturvalliseen työskentelytapaan.

Haastateltavien vastauksista käy ilmi, ettei työnantaja ole järjestänyt tietoturvaan liittyvää koulutusta kuin yhdelle tietoturvasta vastaavalle osastopäällikölle. Yksi haastateltavista oli hakeutunut omaehtoiseen koulutukseen ja kaksi piti tietoturvaan liittyvää koulutusta tarpeellisena.

> *Ei kunnan järjestämänä oo, mutta olen suorittanut niitä vähän muussa vapaaehtoisissa oppilaitoksissa mutta ei oo kunnassa ollut sillaan kauheasti … tietysti jossain palavereissa vähän ohimennen sivuttu mutta minun mielestä se on niinku liian vähäistä se koulutus.* (V1)

> *No minä oon kyllä saanu käyä koulutusta, tietenki itte oon esittäny. No tämän projektin aikana, missä me päästiin tämän xx kanssa siihen, siinähän tuli koulutusta. Mutta minä oon myös*

> *käyny tuota sekä kuntaliiton että jonkun tietoturvasta vastaavien tämmösten yritysten niien koulutuksessa. Ainakin Oulussa ja Rovaniemellä olen käyny.* (V2)

> *No ei ihan nyt muista. Mutta että mä oon vastannu johonkin tän tyyppiseen kysymykseen, mä sanon että aivan liian vähän, eli se on semmonen todella kehitettävä alue ja alue, johon pitää panostaa. Tarvitaan koulutusta.*(V3)

Osastopäälliköiden omassa toiminnassa alaistensa suuntaan tietoturva-asioista tiedottaminen ja niiden esillä pitäminen on painottunut osastopalavereihin. Varsinaista suunnitelmaa tietoturvaan liittyvien asioiden tiedottamisessa ei ole ollut, vaan asiat ovat nousseet esille mm. keskusjohdon kautta. Organisaation intranet on myös toiminut tiedotuskanavana tietoturva-asioissa. Yksi haastateltavista piti oman osastonsa tilannetta tietoturvasta tiedottamisen osalta hyvänä. Muiden näkemysten mukaan tiedottamisessa olisi parantamisen varaa.

> *Kieltämättä parantamiseen varaa aiheessa on muuta on tota on niistä keskusteltu sillon kun niitä asioita on nostettu tuota keskusjohdon kautta esille. Mutta yyyy… tietysti enempi toivos semmosta asiantuntevaa opastusta kuin että tietys meilläkin osastopäälliköillä on tietys vastuut ja velvoitteet että mitä asioita pidetään esillä mutta kehotetaan lukemaan intranettiä että siellä on ohjeita.* (V1)

> *Mä oon ottanu tuota…tuossa osastopalaverissa. Varmaan niihin aikoihin ko oli just tää juttu. Että nythän… ja sama varmaan tuossa riskien kartotuksen yhteydessä tuli keskusteltua näistä. Ja täällä sitten kans että tässä meiän tämmönen kokoontuminen. Mut ei varmaan riittävän paljon. Meiän osastopalaverit on pyritty pitämään silläail, et ne olis kerran kuukaudessa.*(V3)

4.4.4 Tietoturvapoikkeaman käsittely tutkimuskohteessa

Esimiesten vastuulla on laiminlyönneistä huomauttaminen ja tietoturvapoikkeamiin puuttuminen. Lisäksi henkilökunnalle on annettava perustason koulutusta tietoturvallisuuden ylläpitämiseksi.

Kunnan tietoturva-asiakirjassa tietoturvapoikkeaman käsittelyyn kiinnitetään huomiota. Siinä raportoinnin ja seurannan avulla varmistetaan tietojenkäsittelyn tapahtuminen annettujen ohjeiden mukaisesti ja ennen kaikkea varmistetaan, että annettuja ohjeita noudatetaan.

Tutkimuskohteessa on laadittu erillinen tietoturvapoikkeaman käsittelyyn liittyvä ohje. Ohjeen yleisenä tavoitteena on tietojärjestelmiin kohdistuvissa tietoturvapoikkeamatilanteessa minimoida tuhot, palauttaa tietojärjestelmät toimintakuntoon, minimoida käyttöhäiriöt ja poikkeaman vaikutukset normaaliin toimintaan. Ohjeessa on annettu toimintaohjeet tietoturvapoikkeamatapaukissa ja siinä on määritelty selkeä vastuunjako poikkeamatilanteista toipumiseksi.

Haastateltavien vastauksista ilmeni, että tietoturvaan liittyviksi poikkeamiksi ymmärrettiin lähinnä tekniset ongelmat. Poikkeamista ilmoitetaan atk-osastolle, joka hoitaa asiat kuntoon. Yksi haastateltavista otti esille käyttäjistä johtuvat tietoturvapoikkeamat.

> *No käsitteenä tuttu, mutta tota sitä ei oo kyllä käytetty, että missähän yhteydessä se niinku loppujen lopuksi tulee.. mutta se että jos on joku semmonen häiriötilanne (poikkeama) niin niin niistä ei kyllä ilimotuksia oo tehty mutta varmaan sellasia poikkeamatilanteita on ollut. Mutta siitä ei ole tarkkoja ohjeita että missä tapauksessa se pitää tehä.* (V1)

> *Ei se meillä niinko täällä. Hirmusestihan me luotetaan atk-pää pitää huolen näistä*. (V3)

4.4.5 Toiminnan jatkuvuuden turvaaminen ongelmatilanteissa

Organisaation tulee laatia tietoturvasuunnitelmat, jotka osoittavat organisaatiolle elintärkeät tietojärjestelmät, niiden toipumistoimet sekä vaatimukset poikkeusolojen valmiudelle.

Haastateltavat pitivät tärkeänä sitä, että kunta varautuu poikkeustilanteisiin laajemmin kuin pelkästään tietoteknisiin ongelmiin keskittymällä. Haastateltavien vastauksissa korostui tietokoneille ja palvelimille tallennetun tiedon varmistaminen. Nämä varmistustoimet hoitaa kunnan atk-osasto. Varsinaista suunnitelmaa tietoturvaongelmista toipumiseksi haastateltavat eivät olleet nähneet ja sitä ei ole käsitelty kunnan johtoryhmässä erillisenä asiana.

> *Tuota … hmm … semmosta suunnitelmaa ei välttämättä mutta se että tietystihän sitten meillähän on niinku varauduttu tämmö-*

> *siin poikkeusoloihin ..että siihen suunnitelmaan varmaankin sisältyy jossakin muodossa … eli kyllähän meillä toiminnat jatkuu vaikka poikkeusoloja syntyy. Se on tietysti varautumista vielä pahempaan kuin pelekästään tietoturvan kaatumiseen. Mutta kyllä ne siellä jossakin muodossa on nostettu esille.* (V1)

> *Ja meillä on niinkotuota ne varmistukset, niin tuota hoietaan tuonne verkon levylle. Ja ne on taitaa nyt olla kahdennettuna.* (V2)

> *No jos kävis niin ikävästi, että tietokoneelta joutuis kaikki tieto hukkaan, niin onhan meillä olennaiset asiat, jos nyt oppilasasioista puhutaan, niin onhan ne paperilla.* (V4)

Kysyin haastateltavilta tilanteesta, jossa esimerkiksi palvelimet kaatuvat. Mitä siinä tapauksessa toimitaan?

> *Joo … semmoseen yksityisityiskohtaan juuri siihen tarkoitukseen… en tiedä onko atk-osasto tehnyt siihen erikseen .. voi olla että niillä on mutta meille ei oo niistä ainakaan kertonut.* (V1)

4.4.5 Tietoturvallisuuden hallintajärjestelmän auditointi

Henkilöstölle tulee luoda koulutusjärjestelmät joiden avulla perehdytään tietoturvaan sekä välttämättömät ohjeistukset sekä valvonta- ja tarkastusmenettelyohjeet tietoturvan ylläpitämiseksi ja kehittämiseksi.

Tutkittavan kohteen tietoturvapolitiikka lähteen siitä, että kunnan tietojen käsittelyä ja tietojärjestelmien tietoturvan tasoa arvioidaan tarvittaessa ulkoisen tarkastuksen avulla. Lisäksi sisäisin tarkastuksin varmistutaan siitä, että tietoturvakäytännöt on ymmärretty.

Haastateltavien vastauksista ilmeni, ettei tietoturvallisuuden hallintajärjestelmän ulkoista auditointia ole tehty. Sen sijaan pienmuotoisia sisäisiä tarkastuksia on tehty. Haastateltavien mielestä ulkopuoliselle tarkastukselle olisi tarvetta.

> *No .. ei varmaan sanan varsinaisessa merkityksessä jatkuvaa prosessia mutta kyllä tietysti varmaan niinko projektityyppisesti voi olla mutta se että tämmöistä prosessia ei oo luotu* (V1)

> *Ei oo varmaan sillä nimellä, mutta me ollaan kyllä suoritettu niinku tuota semmosia pienempimuotosia kartotuksia.* (V2)

> *Elikkä sillähän pyritään siihen, että tää tietoturva ois standardi ja soveltavan lainsäädännön mukaista, tunnistettujen turvavaatimusten mukaisia ja vaikuttavasti toteutettuja ja ylläpidettyjä ja että ne toimis vielä sitten odotusten mukaisesti. Että semmosiaki kannattaisi tehä ja varmaan sitten tän päätötyön tuloksena jotakin tällaista vois ehkä kuvitellaki.* (V3)

4.5 Etätyö ja tietokoneen matkakäyttö

Etätyön avulla työaikoihin saadaan joustavuutta ja työteho kasvaa. Etätyön avulla perhe-elämä ja työ saadaan paremmin yhteen sovitettua. Etätyön tekeminen parantaa työelämän laatua

Tutkimuskohteessa on laadittu ohje etätyöntekijälle. Ohje kiinnittää huomiota niihin tietoturvallisuusasioihin, joihin etätyötekijällä on mahdollisuus vaikuttaa. Etätyöntekijän omat toimet ratkaisevat tietoturvallisuuden tason. Ohjeessa asetetaan lähtökohdaksi se, että etätyön tekemisen tulee olla yhtä turvallista kuin työn tekeminen kunnan toimistossa. Ohjeessa todetaan, että etäyhteys yksittäisestä verkon ulkopuolisesta työasemasta ei ole toistaiseksi sallittua kunnan verkkoon. Ohjeessa esitellään myös tekniset ratkaisut, jotka mahdollistaisivat etätyön tekemisen tulevaisuudessa.

Haastateltavat tiesivät sen, että kunnan verkkoon ei voi liittyä ulkopuolelta yksittäisellä työasemalla.

> *Se on niinku kielletty kunnan ulkopuolelta tulla tähän kunnan verkkoon esim. vaikka ois kunnan henkilöstöä. Eli se on käytännössä kielletty. Yhteydet on sähköpostitasolla ja Internetin puolla liikkumista mutta kunnan sisäisin järjelyin niihin ei ole päästy.* (V1)

Haastateltavista yksi nosti esille tietokoneen matkakäytön. Muutamilla johtavilla viranhaltijoilla on mahdollisuus työskennellä kannettavan tietokoneen avulla muuallakin kuin kunnan toimistolla.

Kaikkien haastateltavien vastauksissa ilmeni, että etätyön tekemiselle ja eteenkin etäyhteyden muodostamiselle olisi tarvetta. Nykyinen tilanne, jossa

etäyhteyden muodostaminen kunnan verkkoon on kielletty, harmittaa haastateltavia.

> *Ei todellakaan pysty tekemään. Mikä on harmi, minusta. Toki tietty ite eilen illallakin varmaan puoli kahdeksalta vai kahdeksalta töistä lähteneenä olishan voinu vaikka tehdä jotakin asioita kotona. Mutta täällä on tietysti työrauha. Mutta minusta se on huono asia, että sitä etätyötä ei voi tehdä. Mä lähden, mulla on vaikka vapaa päivä, lähden Helsinkii kokoukseen. Mulla olis aikaa tehdä omia töitä, vaikka mä oon vapaapäivällä ja muutenki. Niin minusta se on – vanhanaikaisesti suhtaudutaan täällä etätyöhön.* (V4)

4.6 Sähköinen asiointi

Sähköisestä asioinnista viranomaistoiminnassa säädetty laki on tullut voimaan vuonna 2003. Sähköinen asiointi on lisääntynyt Suomen kunnissa. Suomen kuntaliitto on ohjeistanut kuntien sähköiseen asiointiin liittyen.

Haastateltavien mielestä sähköinen asiointi ja sähköiset palvelut tulevat lisääntymään koko ajan.

> *Sähköiset palvelut lisääntyy huomattavasti koko ajan ja tietysti se tuota parantaa tiedon jakamisen mahdollisuutta. Tällä hetkellä kunnan internetsivuja uusitaan, en tiijä pareneeko ne, mutta se että miten pystytään hyvin lisäämään ja sitten sitä palavelutarjontaa ja minun mielestä se tulee huomattavasti lisääntymään.* (V1)

Yhden haastateltavan vastauksessa otettiin esiin viranomaistoiminta ja sen aiheuttamat haasteet. Haasteista mittavin on sähköinen tunnistaminen.

> *Noo..kyllähän kaikki materiaali, lupahakemukset esim. vois jatkossa ne todennäköisesti tuleekin sähköisessä muodossa kun siihen vaan saadaan sähköiset allekirjoitukset .. saatas virallista dokumenttia että sitten voidaan ottaa niitä käsittelyyn.. edellyttää tämmöstä ns. sähköstä allekirjotusmahdollisuutta.* (V1)

Kunnan tulee haastateltavien mielestä olla mukana kehittämishankkeissa, jotka tukevat sähköisen asioinnin kehittämistä ja käyttöönottoa.

> *Minä nään, et sitä pitäis ehottomasti meillä päästä mukkaan siihen, mutta ku nyt mä oon huomannu, että niin Kela, verottaja, nämä valtion,…nämä ovat niinku hirviästi lisänneet tätä sähköis-*

> *tä palvelua. Mutta nythän siellä onkin niinku kuntaliitoon toimesta niin tämmönen sähköinen asiointi* (V2)

> *Joo se tunnistaminenhan siinä onki. Muttatuota, miten se sitten nämä henkilökortit, kuhan ne tullee, niin onko se sitten ihan aukoton. Tänä päivänähän kaikki järjestelmät nyt näyttäis että pankkitunnuksilla tunnistaudutaan. Mutta eihän sekkään oo. Niin esimerkiksi nythän pystyy sähköpostilla jonku hakemuksen laittamaan, jos se on eheys, siitä voijaan kattoa.* (V3)

Haastateltavien vastauksista voi päätellä, että kunnan tarjoamat sähköiset palvelut ovat koko ajan lisääntymässä. Kuntalaisille tarkoitettujen lomakkeiden määrä on kasvussa. Lomakkeet voi tulostaa ja panna niiden avulla asioita vireille. Varsinaiseen sähköiseen viranomaistoimintaan esteenä on sähköiseen tunnistamiseen liittyvät ongelmat.

> *Kyllä. Kyllä nyt aika pitkälle niinko voi nykyään sähköisesti asioida. Meilläki on lomakkeita… tuolla… netissä, täytettävänä, joita voi täyttää ja hakea sillätavalla. Samoin henkilökunta, ku nuita etuuksia hakkee. Se on hirmusen käytännöllinen tapa.* (V4)

> *Se on sitten ehkä se pullonkaula. Kun ei oo kukaan sanonut, että mikä on se mekanismi, millä nyt tiedetään, että se varmasti olet sinä, joka siellä olisi asioimassa. Ja se on nyt ollu semmonen, joka estää tätä kehitystä, tällä sähköisten palveluiden puolella.* (V4)

5 JOHTOPÄÄTÖKSET

5.1 Toimenpide-ehdotukset

Tutkimustulokset osoittavat, että tietoturvasta vastaavien osastopäälliköiden tiedot tietoturvan eri osa-alueista ovat osittain puutteellisia.

Tämä on huolestuttava havainto, koska mm. Hakalan, Vuorisen ja Vainion (2006) mukaan tietoturva on erittäin laaja kokonaisuus ja se halutaan usein jakaa pienempiin osiin. Näin siitä saadaan helpommin käsiteltäviä osia. Samalla näistä osa-alueista laadittavista dokumenteista saadaan rakenteeltaan selkeämpiä. (Hakala ym. 2006, 10–12.)

Kunnan tietoturvapolitiikkaan liittyvien ohjeistojen (Kohdekunta 2007b) parempi sisäistäminen vaatii tietoturvan eri osa-alueiden tuntemista. Osastopäälliköille tulee järjestää tietoturvaan liittyvää koulutusta työnantajan toimesta. Samalla heitä tulee kannustaa omaehtoiseen tietoturvakoulutukseen.

Tutkimuskohteessa on otettu hyvin huomiin standardin SFS 27001 (2006) hallinnolliselle tietoturvalle asetetut vaatimukset. Päätöksentekojärjestelmä, vastuunjako tietoturvan osalta sekä riskien arvioinnin osalta ovat selkeitä. Hallinnollisen tietoturvan tueksi laaditun ohjeiston avulla osastopäälliköiden on hyvä toteuttaa johtamisessaan tietoturvapolitiikalle asetettuja tavoitteita. (SFS 27001 2006, 14–20; Kohdekunta 2007b.)

Kunnan tietoturvapolitiikka tulee päivittää säännöllisesti ottaen huomioon mahdollisen sähköisen asioinnin lisääntyminen ja etätyömahdollisuuden käyttöönotto sekä Euroopan unionin tietoturvaan liittyvä lainsäädäntö, jota tässä tutkimuksessa ei ole käsitelty. Edellinen tietoturvakartoitus on vuodelta 2007, joten sen päivittäminen tulee ajankohtaiseksi lähivuosina.

Osastopäälliköt tunsivat hyvin tietoturvaan liittyvän vastuunjaon omassa organisaatiossaan.

Tutkimuskohteessa tietoturvapolitiikasta vastaa kunnanhallitus yhdessä kunnanjohtajan kanssa. Kunnanhallitus yhdessä kunnan johdon kanssa määrit-

tävät tietoturvapolitiikan avulla tietoturvallisuuden tavoitteet, vastuut ja toteutuskeinot. Kunnanhallitus on vahvistanut nämä periaatteet 29.5.2007. (Kohdekunta 2007a.)

Osastopäälliköt ymmärsivät myös sen, että hallinnollinen tietoturva on osa kunnan laatujärjestelmää ja riskienkartoitusohjelmaa.

Tutkimuskohteessa kunta on toteuttanut yhdessä konsulttiyhtiön kanssa tietoturvan hallinnan- ja kehittämisprosessin vuosien 2005–2007 aikana. Tietoturvan hallinta on osa kunnan laatujärjestelmää ja hankkeen tavoitteena on ollut nostaa henkilöstön tietoturvan hallinnan tasoa ja tehdä kattava tietoturvakartoitus. Hankkeen tavoitteena on ollut toteuttaa koko kunnan organisaatiota koskeva tietoturvan hallinnan järjestelmä. (Kohdekunta 2007b.)

Tietoturvapolitiikkaan liittyvät ohjeistot, lukuun ottamatta Tietoturvan huoneentaulua ja Etätyöohjetta, olivat osastopäälliköille vieraampia. Nämä ohjeistot antavat osastopäälliköille eväät hyvään ja johdonmukaiseen tietoturvajohtamiseen päivittäisessä toiminnassa.

Osastopäälliköt tulee velvoittaa tutustumaan laadittuihin ohjeisiin ja lisäksi johtoryhmätasolla tulee ottaa ko. ohjeistot esille määräajoin.

Tutkimuskohteessa on laadittu tietoturvapolitiikkaan liittyen seuraavat ohjeistot; Tietojärjestelmien hallinnointi, Tietoturvaohje, Tietosuojaohjeisto, Tietojen ja asiakirjojen luokittelu, Etätyöohje, Tietoturvapoikkeaman käsittely ja Tietoturvallisuuden huoneentaulu. (Kohdekunta 2007b.)

Tietoturvaan liittyvää koulutusta tulee järjestää säännöllisesti sekä osastopäälliköille että muulle henkilöstölle kuten standardi SFS 27001 (2006) ja kunnan oma ohjeistus edellyttävät. Työnantajan tulee luoda henkilöstön koulutusjärjestelmät liittyen tietoturvaan (SFS 27001 2006, 14–20). Tällä hetkellä koulutustoiminta ei ole suunniteltua eikä säännöllistä.

Tietoturvapolitiikan jalkauttamiseksi osaksi henkilöstön jokapäiväistä työtä kuuluu osastopäälliköiden tehtäviin. Tietoturva-asioita on käsitelty henkilös-

töpalavereissa. Käsiteltävä aiheet ovat olleet sellaisia, jotka ovat nousseet esille kunnan johtoryhmätyöskentelyssä.

Asioiden käsittelyn tulee olla suunnitelmallista ja säännönmukaista. Tietoturvastandardin SFS 27001 (2006) mukaan on oleellista, että käyttäjät tietävät ja ymmärtävät ne periaatteet, joille organisaation tietoturvallisuus rakentuu. Tätä varten organisaation johdon tulee julkaista organisaation tietoturvapolitiikka. Politiikka jaetaan koko henkilökunnalle. (SFS 27001 2006, 14–20.)

Kunnan johtoryhmän tulee laatia suunnitelma, jonka avulla organisaation tietoturvapolitiikka esitellään koko henkilökunnalle. Sopivia tilaisuuksia tähän ovat henkilöstöpalaverit ja erilliset koulutustapahtumat.

Tutkimustulokset osoittavat, että kunnan organisaatiossa on tarvetta ja halua tehdä etätyötä. Tietokoneen matkakäyttö on jo osa arkirutiineja. Etätyötä varten on laadittu Etätyöohje (Kohdekunta 2007c). Etätyön tekeminen ei kuitenkaan ole mahdollista, koska kunta ei salli kirjautumisia sisäiseen verkkoon ja tietojärjestelmiin verkon ulkopuolelta.

Etätyön avulla halutaan parantaa työn tuottavuutta ja työelämän laatua. Työssä jaksaminen, työn ja perhe-elämän yhteensovittaminen, työ- ja asuinpaikan joustava sijoittuminen ovat myös merkittäviä etuja puhuttaessa etätyöstä. Etätyön tekeminen vähentää matkakustannuksia ja siihen käytettävää aikaa. (Työ- ja elinkeinoministeriö 2010.)

Kunnassa kannattaa tehdä kartoitus, jolla selvitetään etätyön todellinen tarve työntekijöiden keskuudessa. Kartoituksen perusteella tulee harkita teknisten edellytysten luomista etäyhteyksien sallimiseksi. Samalla tulee ottaa käyttöön toimintasuunnitelma ja toimintaohjeet, jotka mahdollistavat etätyön tekemisen. Tietokoneen matkakäyttöön on laadittava selkeät ohjeet tietoturvan takaamiseksi, koska työnantajan tulee määritellä ne toimintaperiaatteet ja turvamekanismit joiden avulla suojaudutaan riskeiltä, joita etätyö ja tietokoneen matkakäyttö saattavat aiheuttaa (SFS 27001 2006, 50).

Sähköinen asiointi on lisääntynyt tutkimuskohteessa ja tutkimus osoitti, että osastopäälliköt haluavat, että kunta on kehittämässä sähköistä asiointia, ja verkon kautta tarjottavia palveluita niin viranomaistoiminnassa kuin muissakin palveluissa.

Laki sähköisestä asioinnista on tullut voimaan vuonna 2003. Se velvoittaa sellaiset kunnat joilla on tarvittavat tekniset, taloudelliset ja muut valmiudet ryhtymään toimenpiteisiin, joilla sähköinen asiointi mahdollistetaan. (Laki sähköisestä asioinnista viranomaistoiminnassa 2003.)

Sähköisen asioinnin uskotaan lisäävän kuntalaisten tyytyväisyyttä kunnallisiin palveluihin. Samalla sen uskotaan tuovan säästöjä kuntatalouteen ja sen avulla varmistetaan palveluiden saatavuus. (HighTech Forum Oulu 2007.)

Kunnan tulee pyrkiä mukaan sellaisiin hankkeisiin, joilla edistetään sähköistä asiointia viranomaistoiminnassa. Verkon kautta tarjottavia palveluita tulee edelleen kehittää ja näin parantaa kuntalaisille suunnattua palvelutarjontaa. Luottamusmiesorganisaation toiminnassa yhtenä pyrkimyksenä voisi olla siirtyminen paperittomiin kokouksiin.

5.2 Pohdinta ja tutkimuksen luottavuuden arviointi

Tutkimuskohteessa kunta on toteuttanut yhdessä konsulttiyrityksen kanssa tietoturvan hallinnan koulutus- ja kehittämisprosessin vuonna 2005–2007. Hankkeen tavoitteena oli nostaa henkilöstön tietoturvan tasoa, tehdä laaja tietoturvakartoitus ja tuottaa koko organisaatiota koskeva tietoturvan hallinnan järjestelmä. Hankkeen toteuttamistapa oli tietoturvastandardin SFS 17799 mukainen. Hankkeen avulla tuotettiin ohjeet tietojärjestelmien hallintaan, tietojen ja asiakirjojen luokitteluun, tietoturvaan, tietosuojaan, tietoturvapoikkeaman käsittelyyn ja etätyöhön.

Kunnassa on selkeä vastuunjako tietoturvapolitiikan toteuttamiseksi. Tämän vastuunjaon mukaisesti tietoturvapolitiikan käytännön toteuttaminen jää osastopäälliköiden vastuulle. Kunnan atk-osasto huolehtii tietoverkoista ja laitteista. Tietoturvapolitiikan jalkauttaminen osaksi koko organisaation jokapäiväistä työntekoa kuluu siis osastopäälliköiden vastuulle.

Tämä tutkimus osoitti mielestäni, että juuri tietoturvan jalkauttamisessa on ollut ongelmia. Ongelmat johtuvat osittain siitä, että vaikka tietoturvapolitiikkaan liittyvät ohjeet ovat asianmukaisia, niitä ei kuitenkaan tunneta tarpeeksi hyvin. Osastopäälliköille ja henkilöstölle suunnattu tietoturvakoulutus on ollut suunnittelematonta ja vähäistä. Tietoturvaan liittyviä asioita on otettu esille osastopalavereissa. Käsitellyt asiat ovat tulleen osastopalavereihin kunnan johtoryhmän kautta aina silloin, kun se on kokenut ne ajankohtaisiksi. Jotta tietoturvapolitiikka saataisiin osaksi kaikkien työntekijöiden arkirutiineja, siitä pitäisi pitää esillä säännöllisesti ja suunnitellusti. Tietoturvaan liittyvää koulutus tulisi järjestää niin esimiehille kuin henkilöstölle säännöllisesti.

Tämän saman ilmiön ovat havainneet mm. Puhakainen väitöskirjassaan vuodelta 2006 sekä Sampsakoski ja Sihvo opinnäytetyössään vuodelta 2007.
Mm. Puhakainen toteaa väitöskirjassaan ja siitä julkaistussa lehtiartikkelissa, että tietotuvallisuudesta vain pieni osa hoidetaan tekniikan avulla. Suurin osa tietoturvallisuudesta hoidetaan henkilöstön tietoturvallisen käyttäytymisen avulla. Henkilöstöä pitää motivoida tekemään pieniä ja tärkeitä tietoturvallisuutta edistäviä toimenpiteitä. Puhakainen on vakuuttunut siitä, että oikeanlaisen koulutuksen lisää henkilöstön motivaatiota tietoturvallisuuteen liittyvissä asioissa. Johdon esimerkki ja säännöllisyys lisäävät henkilöstön motivaatiota. Koulutus, eli henkilöstön opastaminen ja innostaminen, pitää hoitaa esimerkiksi johdon ja henkilöstön välisissä keskusteluissa, ryhmäpalavereissa, kehityskeskusteluissa ja muissa arkipäivän tilanteissa. Motivaatiota täytyy ylläpitää ottamalla tietoturvatoimenpiteet säännöllisesti esille arjen työelämässä. Johdon tulee itse näyttää esimerkkiä tietoturvallisesta käyttäytymisestä omissa toimissaan. (Puhakainen 2006; Koskivirta 2006.)

Sampakosken ja Sihvon päättötyön yhteenvedossa vuodelta 2006 todetaan, että tutkittavassa kohteessa tietämys tietoturvaan liittyvissä aisoissa suhteellisen vähäistä ja että henkilöstölle pitäisi järjestää koulutusta tietoturvallisuudesta. (Sampasakoski–Sihvo 2007, 26.)

Tutkimuksessani todettiin, että sähköinen asiointi on lisääntynyt Suomessa ja myös tutkimuskohteessa ja, että haastateltavien osastopäälliköiden suhtautuminen sähköisten palveluiden kehittämiseen oli myönteinen.

Asenteen merkitys kunnan sähköisiä palveluita kehitettäessä nousee esille myös Toivasen väitöskirjassa Sähköisten asiointipalvelujen kehittäminen kunnissa (2006). Hän toteaa, että sähköisten asiointipalveluiden merkitys kuntien palvelutuotannossa on vielä vähäinen ja vakiintumaton. Useat kunnat vierastavat informaatioteknologian soveltamista palvelutuotannossa. Suurimmat erot kuntien kehityksessä liittyen sähköiseen asiointiin eivät ilmene niinkään tuotettujen palveluiden määrässä tai laadussa, vaan informaatioteknologian mahdollisuuksien ja sen roolin ymmärtämisessä, asenteissa sekä näiden muokkaamisessa sähköisen palvelutuotannon motiiveissa. (Toivanen 2006.)

Tutkimuksen kohdejoukko vaikuttaa siihen, voidaanko haastattelua käyttää tutkimusmenetelmänä. Kun haastatteluun on päädytty, kohdejoukko määrää sen, millainen haastattelu valitaan tutkimusmenetelmäksi. Haastattelututkimus tehdään tavallisesti satunnaisesti valitusta otoksesta. Satunnaisotantaa yleensä suositellaan, mutta eräät tutkijat vastustavat sitä. Heidän mielestään haastateltavaksi pitää valita sellaisia henkilöitä, jotka tuntevat hyvin haastattelun kohteen. (Hirsjärvi–Hurme 1980, 72.)

Tutkimuksessani haastattelin tutkimuskohteen osastopäälliköitä, jotka vastaavat tietoturvapolitiikan käytännön toteuttamisesta tutkimuskohteessa. Heidän tehtävänä on parantaa henkilöstön tietoturvallisia työskentelytapoja.

Haastattelututkimuksen toteuttamisessa tutkimuksen laadun tarkkailuun tulee kiinnittää huomiota koko tutkimuksen teon ajan. Aineiston luotettavuus on riippuvainen laadusta. Laatuun voidaan vaikuttaa monella eri tavalla tutkimuksen valmisteluvaiheessa ja tutkimuksen aikana. Hyvän haastattelurungon laatiminen ja mahdollisten lisäkysymysten miettiminen etukäteen parantaa haastattelun laatua. Haastatteluista nauhoitettuja nauhoja voidaan kuunnella moneen kertaan ja tarkkailla tutkimuksen laadun kehittymistä niiden kautta. Toimiva tekninen välineistö ja sen ajoittainen tarkastaminen ovat perusasioita pyrittäessä hyvään laatuun. (Hirsjärvi–Hurme 2001, 184–185.)

Suoritin tätä tutkimusta varten haastattelut henkilökohtaisesti, yksi haastateltava kerrallaan. Haastattelussa käytettävään tilaan kiinnitin huomiota siten, että haastateltavat saivat itse valita tilan jossa haastattelu suoritettiin. Haastateltavat valitsivat haastattelupaikaksi oman työhuoneen eli heillä oli haastattelutilanteessa ns. kotikenttäetu. Haastattelu tulee tehdä haastateltavan kotikentällä, jotta sillä on parempi mahdollisuus onnistua (Aaltola–Valli 2001, 28.) Haastattelun luotettavuuteen pyrin vaikuttamaan sillä, että muotoilin teemahaastattelun rungon sellaiseksi, joka kattaa mahdollisimman laajasti tutkimuskysymykset. Käytössäni oli tallennin, jolla tallensin haastattelut. Litteroin haastattelut myöhempää analysointia varten ja tallensin ne omalle tietokoneelleni.

Haastattelujen sisällön analysoinnin luotettavuuteen vaikuttavat tutkija itse, aineiston laatu ja sen analyysi sekä tutkimustulosten esittely. Aineiston ja tutkimustulosten välinen yhteys on analyysissä tärkeää. Keskeinen haaste on, miten pystyy pelkistämään ja tiivistämään aineistoa niin, että se kuvaa mahdollisimman luotettavasti tutkittavaa ilmiötä. (Latvala–Vanhanen–Nuutinen 2003, 36.)

Tutkimusprosessin aikana tehtävät ratkaisut ovat merkittäviä eettisyyden näkökulmasta katsottuna. Tutkijan pitää ottaa kantaa siihen, voidaanko mitä tahansa aihetta tutkia tai millaista on hyvän tieteellisen käytännön mukainen tutkimus. Pohdittavia asioita ovat myös tutkijan vastuu siitä, mihin hänen tuottamaansa tutkimustietoa käytetään. (Saaranen-Kauppinen & Puusniekka 2006.)

Tutkimukseni toimeksiantajana oli tutkittavan kunnan virkamiesjohto, joka halusi tutkittua tietoa tietoturvajohtamisesta oman toimintansa kehittämiseksi. Tutkimustulokset ovat julkisia, koska tutkimuksen lähdemateriaalina olleet salaiset tietoturvaan liittyvät ohjeet ovat kunnan hallussa ja eikä niistä julkaistu sellaisia kohtia, joista olisi haittaa kunnan tietoturvalle tai muulle toiminnalle.

Työssään tutkija käyttää asiantuntijavaltaa. Erityisesti ihmisiin kohdistuvan tutkimuksen tekeminen edellyttää tutkijalta tutkittavan ihmisarvon ja itsemää-

räämisoikeuden kunnioittamista. Kun tutkija käyttää hyvin standardoituja tiedonkeruumenetelmiä, ovat mahdolliset tutkimusasetelmaan liittyvät eettiset ongelmakohdat ennakoitavissa ja etukäteen ratkaistavissa. (Saaranen-Kauppinen & Puusniekka 2006.)

Tutkimukseni tiedonkeruumenetelmänä oli teemahaastattelu, johon tutkittavat henkilöt osallistuivat vapaaehtoisesti ja he itse saivat päättää haastatteluajan ja -paikan. Haastattelut ja siitä kertynyt äänitetty materiaali sekä haastattelujen litteroinnit hävitetään heti, kun niitä ei tutkimuksen raportoinnissa tarvita.

LÄHTEET

Aaltola, J. – Valli, R. 2001. Ikkunoita tutkimusmedoteihin 1. PS-kustannus. Gummerus. Jyväskylä.

Arkistolaki. 1984. L 831/1994.

Enberg M. 2002. Kuntien riskinhallinta. Suomen Kuntaliitto. Osoitteessa http://www.kunnat.net/binary.asp?path=1;29;356;70728;11322;12073;12074&field=FileAttachment&version=5. 18.1.2011.

Eskola, J. – Suoranta, J. 1996. Johdatus laadulliseen tutkimukseen. Lapin yliopisto.

Grönfors, M. 1982. Kvalitatiiviset kenttätyömenetelmät. WSOY. Helsinki.

Hakala, M. – Vainio, M. – Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Ohjeistus, toteutus ja lainsäädäntö Jyväskylä: Docendo Finland Oy.

Henkilötietolaki. 1999. L 523/1999. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/1999/19990523. 18.1.2011.

HighTech Forum Oulu. 2007. Sähköinen asiointi lisääntyy kunnissa . Osoitteessa http://www.hightechforum.fi/index.cfm?j=687399. 4.5.2011.

Hirsjärvi, S. – Hurme, H. 1980. Teemahaastattelu. Gaudeamus. Tammer-Paino Oy, Tampere.

Hirsjärvi, S. – Hurme, H. 2001. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Kustannusosakeyhtiö Tammi. Helsinki.

ISO 27000 Directory. 2009. The ISO 27000 Directory. Osoitteessa http://www.27000.org. 30.1.2011.

ISO 27001 Sertifiointi. 2011. Bureau Veritas Finland. Osoitteessa http://www.bureauveritas.fi/wps/wcm/connect/bv_fi/Local/Home/bv_com_serviceSheetDetails?serviceSheetId=13532&serviceSheetName=ISO+27001+sertifiointi. 2.2.2011

Kettunen, E. 2010. Kuntien ja kuntayhtymien tietotekniikkakartoitus. Suomen kuntaliitto. Osoitteessa http://www.kuntaportaali.org/binary.asp?path=1;29;1042;163602field=FileAttachment&version=2. 4.5.2011.

Kohdekunta. 2007a. Kunnanhallituksen päätös 147§.

Kohdekunta. 2007b. Kunnanjohtajan yleispäätös 4§.

Kohdekunta. 2007c. Etätyöohje.

Kohdekunta. 2007d. Kunnan tietoturvapolitiikka.

Kohdekunta. 2007e. Tietoturvapoikkeaman käsittely.

Koskivirta, P. 2006.. Näin motivoit henkilöstön käyttäytymään tietoturvallisesti. Turvallisuus-lehti 3/2006. Helsinki.

Kuntaliitto 2011a. Riskienhallinnan järjestäminen ja riskien arviointi. Osoitteessa http://www.kunnat.net/binary.asp?path=1;29;356;70728;11322;12058;12060&field=FileAttachment&version=3. 18.1.2011.

Kuntaliitto 2011b. Konserniohje. Osoitteessa http://www.kunnat.net/binary.asp?path=1;29;347;93749;108318;11443;83718&field=FileAttachment&version=5. 18.1.2011.

Kuntatyönantajat. 2010. Työelämän kehittäminen. Osoitteessa http://www.kuntatyonantajat.fi/fi/tyoelaman-kehittaminen/etatyo/Sivut/default.aspx. 4.5.2011.

Krutz, R. – Vines, R. 2003. (Käännös Suominen E.) Tietoturvasertifikaatti, CISSP. Helsinki. IT Press.

Kylmä, J. – Juvakka, T. 2007. Laadullinen terveystutkimus. Edita Prima Oy. Helsinki.

Laki kunnallisesta viranhaltijasta. 2003. L 304/2003. Osoitteessa http://www.finlex.fi/fi/laki/kokoelma/2003/20030048.pdf. 18.1.2011.

Laki yksityisyyden suojasta työelämässä. 2001. L 477/2001. Osoitteessa http://www.finlex.fi/fi/laki/kokoelma/2001/20010071.pdf. 18.1.2011.

Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta. 1999. L 565/1999. Osoitteessa http://www.finlex.fi/fi/laki/kokoelma/1999/19990060.pdf. 18.1.2011.

Laki sähköisestä asioinnista viranomaistoiminnassa. 2003. L 618/2003. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/2003/20030013. 4.5.2011

Laki viranomaisten toiminnan julkisuudesta. 1999. L 621/1999. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/1999/19990621. 18.1.2011.

Laaksonen, M. – Nevasalo, T. – Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö Helsinki: Edita.

Latvala, E. – Vanhanen – Nuutinen, L. 2003. Laadullisen hoitotieteellisen tutkimuksen tutkimusprosessi. Sisältöanalyysi. WSOY. Helsinki.

Metsämuuronen, J. 2000. Laadullisen tutkimuksen perusteet. Methelp International Oy. Helsinki.

Metsämuuronen, J. 2005. Tutkimuksen tekemisen perusteet ihmistieteissä. Gummerus. Jyväskylä.

Perustuslaki. 1999. L 731/1999. Osoitteessa http://www.finlex.fi/fi/laki/kokoelma/1999/19990074.pdf. 18.1.2011.

Pfleeger, C. – Pfleeger, S. 2003. Security in Computing, Third Edition, Pearson Education Inc. Prentice Hall Professional Technical Reference, New Jersey.

Puhakainen, P. 2006. A design theory for information security awareness. Oulun yliopisto.

Rikoslaki. 1889. L 39/1889.

Saaranen-Kauppinen, A. – Puusniekka, A. 2006. KvantiMOTV - Menetelmäopetuksen tietovaranto. Tampere : Yhteiskuntatieteellinen tietoarkisto. http://www.fsd.uta.fi/menetelmaopetus. 10.5.2011

Sampsakoski, I. – Sihvo, J. 2006. Tietoturvaohjeistus case: Vapaa Valinta, Tampereen ammattikorkeakoulu. Liiketalous.

SFS 17799. 2006. ISO/IEC 17799 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Helsinki. Suomen Standardisoimisliitto SFS.

SFS 27001. 2006. ISO/IEC 27001 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje.Helsinki. Suomen Standardisoimisliitto SFS.

SFS 27002. 2007. ISO/IEC 27002 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Suomen Standardisoimisliitto SFS.

Suomen kuntaliitto. 2010. Sähköinen asiointi. Osoitteessa http://www.kuntaportaali.org/k_perussivu.asp?path=1;29;349;103182;115325. 4.5.2011.

Suomen kuntaliitto. 2003. Sähköisen asioinnin uudistus. Osoitteessa http://www.kunnat.net/fi/Kuntaliitto/yleiskirjeet-lausunnot/yleiskirjeet/2003/Sivut/y6802003-sahkoisen-asioinnin-uudistus.aspx. 4.5.2011.

Toivanen, M. 2006. Sähköisten asiointipalvelujen kehittäminen kunnissa. Akateeminen väitöskirja. Tampereen yliopiston kauppa- ja hallintotieteiden tiedekunta. Tampere.

Työ- ja elinkeinoministeriö. 2010. Työlainsäädäntö. Osoitteessa: http://www.tem.fi/index.phtml?s=2387. 4.5.2011

Työsopimuslaki. 2001. L 55/2001. Osoitteessa http://www.finlex.fi/fi/laki/kokoelma/2001/20010010.pdf. 18.1.2011.

Vahingonkorvauslaki 1974. L 41/1974.

Valtion virkamieslaki.1994. L 750/1994.

Valtiovarainministeriö. 2011.Tietoturvaopas, Tietoturvallisuus Suomen lainsäädännössä. Osoitteessa http://www.yliopistojentt.fi/VAHTI-CD/Sivusto/lait/suomessa.htm. 18.1.2011.

Viestintävirasto. 2009. Tietoturvalliseen yhteiskuntaan. Osoitteessa http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html. 1.2.2011.

VirtuaaliAMK. 2011 Liiketoiminnan kehittäminen, Tietoturvan osa-alueet. Osoitteessa http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html. 14.4.2011.

Yhteiskunnan Tieto – Knowledge of Society. 2008. ISO/IEC Riskienhallinta standardi. Osoitteessa http://www.yhteiskunnantieto.fi/ajankohtaista_iso27005.pdf. 18.1.201

LIITTEET

Tietoturvasta vastaavien osastopäälliköiden haastattelurunko. Liite1.

Liite 1. Tietoturvasta vastaavien osastopäälliköiden haastattelurunko.

Haastattelun runko

Haastattelun avulla pyrin selvittämään osastopäälliköiden tietoturvakysymyksiin liittyvän tietämyksen eli johdon sitoutumisen organisaation tietoturvapolitiikkaan ja sen, miten on toteutettu koulutus- ja tietoisuusohjelmat, joiden avulla tietoturvapolitiikka jalkautetaan henkilötön piiriin. Haastattelu perustuu tietoturvastandardiin ISO/IEC 27001.

1) Tarkoituksena on saada kokonaiskuva osastopäälliköiden tietoturva-asioiden hallinnasta ja
2) tietoturva-asioiden jalkauttamisesta henkilökunnalle sekä
3) kartoittaa osastopäälliköiden kehittämistarpeet/-ideat liittyen tietoturvan jalkauttamiseen.

Seuraavat kysymykset kartoittavat osastopäälliköiden tietämystä tietoturvasta.

Miten ymmärrät käsitteen tietoturva?
(Hallinnollinen turvallisuus, fyysinen turvallisuus, henkilöturvallisuus, tietoaineistoturvallisuus, ohjelmistoturvallisuus, laitteistoturvallisuus, tietoliikenneturvallisuus)

Mitä kunnan tietoturvaan/tietoturvapolitiikkaan liittyviä ohjeistoja tunnet?
(Tietojärjestelmän hallinnointi, tietoturvaohje, tietosuojaohjeisto, tietojen ja asiakirjojen luokittelu, etätyöohje, tietoturvapoikkeaman käsittely, sekä tietoturvallisuudenhuoneentaulu.)

Kuka vastaa tietoturvapolitiikasta ja tietoturvasta kunnassa?

Mitä koulutusta kunta on järjestänyt sinulle tietoturvasta?

Mitä koulutusta olisi mielestäsi pitänyt järjestää?

Onko kunnassa suoritettu tietoturvallisuuden hallintajärjestelmän sisäisiä auditointeja?

(Organisaation tulee suorittaa tietoturvallisuuden hallintajärjestelmän sisäisiä auditointeja suunnitelluin aikavälein määrittääkseen, ovatko teitoturvallisuuden hallintajärjestelmän valvontavelvoitteet, turvamekanismit, prosessit ja menettelutavat:

- *standardin ja soveltavan lainsäädännön mukaiset*
- *tunnistettujen tietoturvavaatimusten mukaiset*
- *vaikuttavasti toteutettuja ja ylläpidettyjä*
- *toiminnassa odotusten mukaisesti)*

Seuraavat kysymykset kartoittavat tietoturvan jalkauttamista

Miten olet tiedottanut tai ottanut esille tietoturvakysymykset alaistesi kanssa.

Onko henkilöstöä/alaisiasi koulutettu tietoturvaan liittyvissä kysymyksissä?

Ovatko alaisesi omaehtoisesti hakeutuneet alan koulutuksiin?

Kehittämistarpeet tietoturvaan liittyen

Miten tietoturvakysymykset saataisiin jalkautettua kentälle osaksi työntekijöiden jokapäiväistä työskentelyä.
Mitkä tavat ja tilaisuudet olisivat mielestäsi luontevimpia tähän tarkoitukseen?
Miten näet etätyön merkityksen nyt ja tulevaisuudessa?
Miten sähköiset palvelut tulevat kehittymään tulevaisuudessa?

Onko sinulla jotain sellaista sanottavaa tietoturvasta, joka ei ole vielä tässä haastattelussa noussut esille?

Olisiko sinulla jotain tarinaa tai tapausta tietoturvaan liittyen, jonka voisit vielä lopuksi kertoa?